112857-411

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月１０日

出願番号
Application Number: 特願２００２－２０１４７２

[ST.10/C]: [ＪＰ２００２－２０１４７２]

出願人
Applicant(s): ソニー株式会社

２００３年　６月　２日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４２４５５

【書類名】　特許願
【整理番号】　0290427104
【提出日】　平成14年 7月10日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
H04L 9/32
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　松山　科子
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100110434
【弁理士】
【氏名又は名称】　佐藤　勝
【手数料の表示】
【予納台帳番号】　076186
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0011610
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　リモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体

【特許請求の範囲】

【請求項１】　所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器と、

上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当する機器であるゲートウェイ機器と、

少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させる上記ゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持し、上記アクセス対象機器に対してアクセスするアクセス機器とを備え、

上記アクセス機器は、上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器は、上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記アクセス対象機器に対して送信して提示し、

上記アクセス対象機器は、上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスシステム。

【請求項２】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器の情報が記述されたものであること

を特徴とする請求項１記載のリモートアクセスシステム。

【請求項３】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の検証者たる上記アクセス対象機器が当該権限及び経由情報記述属性証明書の所有者を認証する場合に利用するサービスに関する認証情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項１記載のリモートアクセスシステム。

【請求項４】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の所有者のアクセス許可情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項１記載のリモートアクセスシステム。

【請求項５】　上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与えるための電子証明書である発行許可情報記述属性証明書を発行する所定の属性認証局を備え、

上記ゲートウェイ機器は、上記属性認証局によって発行された上記発行許可情報記述属性証明書に基づいて、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して発行すること

を特徴とする請求項１記載のリモートアクセスシステム。

【請求項６】　上記発行許可情報記述属性証明書は、当該発行許可情報記述属性証明書の所有者たる上記ゲートウェイ機器に与えられる役割を示すロール情報として、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与える旨を示す情報が記述されたものであること

を特徴とする請求項５記載のリモートアクセスシステム。

【請求項７】　公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局を備え、

上記属性認証局は、上記証明書発行認証局とは異なるローカルな機関であること

を特徴とする請求項５記載のリモートアクセスシステム。

【請求項８】　上記証明書発行認証局は、上記アクセス対象機器、上記ゲートウェイ機器、及び上記アクセス機器のそれぞれに対して上記公開鍵証明書を発行

すること

を特徴とする請求項７記載のリモートアクセスシステム。

【請求項９】　上記権限及び経由情報記述属性証明書は、上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属するエンティティによって発行されたものであること

を特徴とする請求項１記載のリモートアクセスシステム。

【請求項１０】　上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属する他のアクセス対象機器と、

上記他のネットワークの入り口に相当する機器である他のゲートウェイ機器と、

上記ゲートウェイ機器がアクセスすることができる上記他のネットワークにおけるエンティティとしての上記他のゲートウェイ機器を示す情報が記述された電子証明書であるゲートウェイ機器情報記述属性証明書を発行する所定の属性認証局とを備え、

上記ゲートウェイ機器は、上記属性認証局によって発行された上記ゲートウェイ機器情報記述属性証明書を上記他のゲートウェイ機器に対して送信して提示し、上記権限及び経由情報記述属性証明書を発行してもらい、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して送信すること

を特徴とする請求項９記載のリモートアクセスシステム。

【請求項１１】　上記アクセス機器は、上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器は、上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器が属する上記他のネットワークにおける上記他のゲートウェイ機器に対して送信して提示し、

上記他のゲートウェイ機器は、上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器に対して送信して提示し、

上記他のアクセス対象機器は、上記他のゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とする請求項１０記載のリモートアクセスシステム。

【請求項１２】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器及び上記他のゲートウェイ機器の両方の情報が記述されたものであること

を特徴とする請求項１０記載のリモートアクセスシステム。

【請求項１３】　上記ゲートウェイ機器情報記述属性証明書は、当該ゲートウェイ機器情報記述属性証明書の所有者のアクセス許可情報として、上記ゲートウェイ機器がアクセスすることができる上記他のゲートウェイ機器を示す情報が記述されたものであること

を特徴とする請求項１０記載のリモートアクセスシステム。

【請求項１４】　公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局を備え、

上記属性認証局は、上記証明書発行認証局とは異なるローカルな機関であること

を特徴とする請求項１０記載のリモートアクセスシステム。

【請求項１５】　上記証明書発行認証局は、上記アクセス対象機器、上記ゲートウェイ機器、上記アクセス機器、上記他のアクセス対象機器、及び上記他のゲートウェイ機器のそれぞれに対して上記公開鍵証明書を発行すること

を特徴とする請求項１４記載のリモートアクセスシステム。

【請求項１６】　所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少な

くとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持させ、

上記アクセス機器によって上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器によって上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記アクセス対象機器に対して送信して提示し、

上記アクセス対象機器によって上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセス方法。

【請求項１７】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器の情報が記述されたものであること

を特徴とする請求項１６記載のリモートアクセス方法。

【請求項１８】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の検証者たる上記アクセス対象機器が当該権限及び経由情報記述属性証明書の所有者を認証する場合に利用するサービスに関する認証情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項１６記載のリモートアクセス方法。

【請求項１９】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の所有者のアクセス許可情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項１６記載のリモートアクセス方法。

【請求項２０】　所定の属性認証局によって発行された電子証明書であり、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与えるための電子証明書である発行許可情報記述属性証明書に基づいて、上記ゲートウェイ機器によって上記権限及び経由情報記述属性証明書を上記アクセス機器に対して発行すること

を特徴とする請求項１６記載のリモートアクセス方法。

【請求項２１】　上記発行許可情報記述属性証明書は、当該発行許可情報記述属性証明書の所有者たる上記ゲートウェイ機器に与えられる役割を示すロール情報として、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与える旨を示す情報が記述されたものであること

を特徴とする請求項２０記載のリモートアクセス方法。

【請求項２２】　上記属性認証局は、公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局とは異なるローカルな機関とされること

を特徴とする請求項２０記載のリモートアクセス方法。

【請求項２３】　上記アクセス対象機器、上記ゲートウェイ機器、及び上記アクセス機器のそれぞれに対して、上記証明書発行認証局によって上記公開鍵証明書を発行すること

を特徴とする請求項２２記載のリモートアクセス方法。

【請求項２４】　上記権限及び経由情報記述属性証明書は、上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属するエンティティによって発行されたものであること

を特徴とする請求項１６記載のリモートアクセス方法。

【請求項２５】　所定の属性認証局によって発行された電子証明書であり、上記アクセス対象機器が属するネットワークとは異なる他のネットワークにおける上記ゲートウェイ機器がアクセスすることができるエンティティとしての当該他のネットワークの入り口に相当する機器である他のゲートウェイ機器を示す情報が記述されたゲートウェイ機器情報記述属性証明書を、上記ゲートウェイ機器に

よって上記他のゲートウェイ機器に対して送信して提示し、上記権限及び経由情報記述属性証明書を発行してもらい、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して送信すること

を特徴とする請求項２４記載のリモートアクセス方法。

【請求項２６】　上記アクセス機器によって上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器によって上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書を、アクセスの対象として指定された上記他のネットワークに属する他のアクセス対象機器が属する当該他のネットワークにおける上記他のゲートウェイ機器に対して送信して提示し、

上記他のゲートウェイ機器によって上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器に対して送信して提示し、

上記他のアクセス対象機器によって上記他のゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とする請求項２５記載のリモートアクセス方法。

【請求項２７】　上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器及び上記他のゲートウェイ機器の両方の情報が記述されたものであること

を特徴とする請求項２５記載のリモートアクセス方法。

【請求項２８】　上記ゲートウェイ機器情報記述属性証明書は、当該ゲートウェイ機器情報記述属性証明書の所有者のアクセス許可情報として、上記ゲートウェイ機器がアクセスすることができる上記他のゲートウェイ機器を示す情報が記

述されたものであること

を特徴とする請求項２５記載のリモートアクセス方法。

【請求項２９】　上記属性認証局は、公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局とは異なるローカルな機関とされること

を特徴とする請求項２５記載のリモートアクセス方法。

【請求項３０】　上記アクセス対象機器、上記ゲートウェイ機器、上記アクセス機器、上記他のアクセス対象機器、及び上記他のゲートウェイ機器のそれぞれに対して、上記証明書発行認証局によって上記公開鍵証明書を発行すること

を特徴とする請求項２９記載のリモートアクセス方法。

【請求項３１】　所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムであって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、

上記アクセス機器から上記ゲートウェイ機器を介して送信されて提示された上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスプログラム。

【請求項３２】　所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムが記録された記録媒体であって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続するこ

とを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、

上記リモートアクセスプログラムは、

上記アクセス機器から上記ゲートウェイ機器を介して送信されて提示された上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスプログラムが記録された記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体に関する。

【０００２】

【従来の技術】

近年、ネットワークに接続可能な情報家電等の各種機器が開発されており、これにともない、家庭内ネットワークをはじめとして様々な機器を対象としたネットワークが構築されつつある。また、このような状況に応じて、屋外等の遠隔地から屋内に設けられた各種情報家電又はパーソナルコンピュータ等の各種情報処理端末若しくはサーバ装置等に対して、ユーザが所持する携帯電話機や携帯情報端末機（Personal Digital Assistants；ＰＤＡ）等の機器を用いてリモートアクセスすることによって享受できるサービスが各種提案されている。

【０００３】

このようなサービスにおいては、当該サービスを提供するサーバ装置等のハードウェアやソフトウェア、さらにはデータといった各種リソースに対する不正なユーザのアクセスを排除すべく、認証及びアクセス権の管理を行うことが必須とされている。

【０００４】

【発明が解決しようとする課題】

ところで、上述したサービスとしては、既に実施されているものもあり、個別に認証の仕組みを構築している。しかしながら、このようなサービスにおいては、個人単位の権限（操作）をも含めた認証方式が未だ確立されていないのが現状である。

【０００５】

また、個人単位の権限管理の手法としては、いわゆるＩＤ（IDentification）パスワードを用いた認証方式があるが、このＩＤパスワードを用いた認証方式においては、仕組みが非常に煩雑となり、処理負担が大きいといった問題があった。

【０００６】

本発明は、このような実情に鑑みてなされたものであり、いわゆる属性証明書（Attribute Certificate；ＡＣ）を用いて権限管理を行うことにより、リモートアクセスを行う際に、リソースにアクセスする機器自体等のエンティティのみならず、アクセスさせたいリソース毎に、権限単位での制御を容易且つ安全に行うことができるリモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上述した目的を達成する本発明にかかるリモートアクセスシステムは、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器と、このアクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当する機器であるゲートウェイ機器と、少なくともリソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持し、アクセス対象機器に対してアクセスするアクセス機器とを備え、アクセス機器は

、権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器は、アクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器は、ゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【０００８】

このような本発明にかかるリモートアクセスシステムは、少なくともリソースに対する権限とゲートウェイ機器の情報とを、権限及び経由情報記述属性証明書に記述し、この権限及び経由情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証する。

【０００９】

また、上述した目的を達成する本発明にかかるリモートアクセス方法は、所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持させ、アクセス機器によって権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器によってアクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器によってゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【００１０】

このような本発明にかかるリモートアクセス方法は、少なくともリソースに対する権限とゲートウェイ機器の情報とを、権限及び経由情報記述属性証明書に記述し、この権限及び経由情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証する。

【００１１】

さらに、上述した目的を達成する本発明にかかるリモートアクセスプログラムは、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【００１２】

このような本発明にかかるリモートアクセスプログラムは、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経由情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経由情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証する。

【００１３】

さらにまた、上述した目的を達成する本発明にかかるリモートアクセスプログラムが記録された記録媒体は、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムが記録された記録媒体であ

って、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、リモートアクセスプログラムは、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【００１４】

このような本発明にかかるリモートアクセスプログラムが記録された記録媒体は、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経由情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経由情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証するリモートアクセスプログラムを提供する。

【００１５】

【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【００１６】

この実施の形態は、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムである。このリモートアクセスシステムは、ＩＳＯ（International Organization for Standardization）／ＩＥＣ（International Electrotechnical Commission）　９５９４－８、又はＩＴＵ－Ｔ　Ｘ．５０９に基づく属性証明書（Attribute Certificate；ＡＣ）を用いて権限管理を行うことにより、リモートアクセスを行う際に、リソースにアクセスする機器自体等のエンティティのみならず、アクセスさせたいリソース毎に、権限単位での制御を容易に

行うことができるものである。また、このリモートアクセスシステムは、属性証明書を利用する際に、リソースが属するネットワークの入り口となるゲートウェイを経由して、リソースとこのリソースにアクセスしようとする機器との間で属性証明書の授受を行うことにより、属性証明書の送付ルートを確認することを可能とし、セキュリティを向上させることができるものである。

【００１７】

まず、リモートアクセスシステムの説明に先だって、当該リモートアクセスシステムにて用いる電子証明書である公開鍵証明書（Public Key Certificate；ＰＫＣ）及び上述した属性証明書の概略について説明する。

【００１８】

まず、公開鍵証明書について説明する。公開鍵証明書は、いわゆる公開鍵暗号方式における独立した所定の第三者機関である証明書発行認証局（Certification Authority；ＣＡ又はIssuer Authority；ＩＡ）によって発行されるものである。

【００１９】

ここで、公開鍵暗号方式について説明する。公開鍵暗号方式は、発信者と受信者との鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵とし、他方の鍵を秘密に保つ秘密鍵とするものである。公開鍵暗号方式は、暗号化及び復号に共通の鍵を用いるいわゆる共通鍵暗号方式と異なり、秘密に保つ必要がある秘密鍵を特定の１人が持てばよいため、共通鍵暗号方式と比較して鍵の管理において有利である。公開鍵暗号方式の代表的なものとしては、いわゆるＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このＲＳＡ暗号は、例えば１５０桁程度の非常に大きな２つの素数の積の素因数分解処理の困難性を利用するものである。

【００２０】

公開鍵暗号方式は、不特定多数のユーザに公開鍵を使用可能とするものであり、配布する公開鍵が正当なものであるか否かを証明するために公開鍵証明書を用いる方法が広く用いられている。例えば、公開鍵暗号方式においては、ある特定のユーザＡが対となる公開鍵と秘密鍵とを生成し、生成した公開鍵を証明書発行

認証局に対して送付して公開鍵証明書を取得し、この公開鍵証明書を一般に公開する。一方、不特定のユーザは、公開鍵証明書に基づいて所定の手続きを経ることによって公開鍵を取得し、平文たる文書等を暗号化して特定のユーザＡに対して送付する。そして、ユーザＡは、不特定のユーザから送付された暗号化文書を秘密鍵を用いて復号する等の処理を行う。公開鍵暗号方式は、このような暗号方式である。

【００２１】

また、公開鍵暗号方式においては、ユーザＡは、秘密鍵を用いて平文たる文書等に署名を付加し、不特定のユーザが公開鍵証明書に基づいて所定の手続きを経ることによって公開鍵を取得し、その署名の検証を行うことが可能となる。例えば、公開鍵暗号方式においては、証明書発行認証局が公開鍵証明書を参照して公開鍵を判別すると、任意の平文たる文書等をユーザＡに対して送付し、秘密鍵を用いて暗号化させ、再度送り返させる。証明書発行認証局は、ユーザＡから送付された暗号化文書を公開鍵を用いて復号することにより、署名の正当性を検証することができる。

【００２２】

このような公開鍵暗号方式における公開鍵証明書は、管理者たるユーザが自己を識別するための情報や公開鍵等を証明書発行認証局に提出することにより、証明書発行認証局側が当該証明書発行認証局を識別するための情報や有効期限等の情報を付加し、さらに証明書発行認証局による署名を付加して作成される。

【００２３】

具体的には、公開鍵証明書は、図１及び図２に示すようなフォーマットから構成される。なお、同図においては、公開鍵証明書を構成する各フィールド毎の項目と、これらの各項目に対する説明とを記載している。

【００２４】

図１に示すバージョン（version）は、公開鍵証明書のフォーマットのバージョン情報を記述するフィールドであり、例えばフォーマットがバージョン３である場合にはバージョン３を示す”２”が記述される。

【００２５】

シリアルナンバ（serial Number）は、証明書発行認証局によって設定される公開鍵証明書のシリアルナンバを記述するフィールドであり、例えばシーケンシャルな番号が記述される。

【００２６】

署名アルゴリズム識別子、及びアルゴリズムパラメータ（signature algorithm Identifier algorithm parameters）は、公開鍵証明書の署名アルゴリズムを識別するための情報とそのパラメータとを記述するフィールドである。署名アルゴリズムとしては、例えば楕円曲線暗号又はＲＳＡ暗号があり、署名アルゴリズムとして楕円曲線暗号が適用されている場合には、アルゴリズムパラメータとしてパラメータ及び鍵長が記述され、署名アルゴリズムとしてＲＳＡ暗号が適用されている場合には、アルゴリズムパラメータとして鍵長が記述される。

【００２７】

発行者（issuer）は、公開鍵証明書の発行者、すなわち、証明書発行認証局の名称を識別可能とする形式（Distinguished Name）で記述するフィールドである。

【００２８】

有効期限（validity）は、公開鍵証明書の有効期限である開始日時（not Before）及び終了日時（not After）を記述するフィールドである。

【００２９】

サブジェクト（subject）は、ユーザである認証対象者の名前を記述するフィールドであり、例えばユーザ機器の識別子やサービス提供主体の識別子等が記述される。

【００３０】

サブジェクト公開鍵情報（subject Public Key Info algorithm subject Public key）は、ユーザの公開鍵情報としての鍵アルゴリズムや鍵情報自体を記述するフィールドであり、鍵アルゴリズムとしては、例えば楕円曲線暗号又はＲＳＡ暗号がある。

【００３１】

これらの各フィールドは、公開鍵証明書のフォーマットがバージョン１以降の

バージョンであるものに含まれるフィールドであり、以下に示す各フィールドは、バージョン３であるものに追加されるフィールドである。

【００３２】

証明局鍵識別子（authority Key Identifier-key Identifier, authority Cert Issuer, authority Cert Serial Number）は、証明書発行認証局の署名確認用の鍵を識別するための情報であり、８進数表記の鍵識別番号、一般名称（General Name）形式の証明書発行認証局の名称、及び認証番号を記述するフィールドである。

【００３３】

サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を記述するフィールドである。

【００３４】

鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（０）ディジタル署名用（digital Signature）、（１）否認防止用（non Repudiation）、（２）鍵の暗号化用（key Encipherment）、（３）メッセージの暗号化用（data Encipherment）、（４）共通鍵配送用（key Agreement）、（５）認証の署名確認用（key Cert Sign）、（６）失効リストの署名確認用（CRL Sign）、（７）鍵交換時（key Agreement）データの暗号化にのみ利用（encipher Only）、及び（８）鍵交換時データの復号にのみ利用（decipher Only）の各使用目的が設定される。

【００３５】

秘密鍵有効期限（private Key Usage Period）は、ユーザが有する秘密鍵の有効期限である開始日時（not Before）及び終了日時（not After）を記述するフィールドであり、デフォルトでは、公開鍵証明書の有効期限と公開鍵の有効期限と秘密鍵の有効期限とは互いに同一とされる。

【００３６】

図２に示す認証局ポリシー（Certificate Policy）は、証明書発行認証局の証明書発行ポリシーを記述するフィールドであり、例えばＩＳＯ／ＩＥＣ　９８３

４－１に準拠したポリシーＩＤ（policy Identifier）や認証基準（policy Qualifiers）が記述される。

【００３７】

ポリシー・マッピング（policy Mappings）は、証明書発行認証局を認証する場合にのみ記述されるフィールドであり、証明書発行を行う証明書発行認証局のポリシー（issuer Domain Policy）と被認証ポリシー（subject Domain Policy）とのマッピングを規定する。

【００３８】

サポート・アルゴリズム（supported Algorithms）は、ディレクトリ（Ｘ．５００）のアトリビュートを定義するフィールドである。サポート・アルゴリズムは、コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。

【００３９】

サブジェクト別名（subject Alt Name）は、ユーザの別名を一般名称（General Name）形式で記述するフィールドである。

【００４０】

発行者別名（issuer Alt Name）は、証明書発行者の別名を記述するフィールドである。

【００４１】

サブジェクト・ディレクトリ・アトリビュート（subject Directory Attributes）は、ユーザの任意の属性を記述するフィールドである。

【００４２】

基本制約（basic Constraints）は、証明対象の公開鍵が証明書発行認証局の署名用であるかユーザのものであるかを区別するためのフィールドである。

【００４３】

許容サブツリー制約名（name Constraints permitted Subtrees）は、被認証者が証明書発行認証局である場合にのみ使用される公開鍵証明書の有効領域を示すフィールドである。

【００４４】

制約ポリシー（policy Constraints）は、認証パスの残りに対する明確な認証ポリシーＩＤや禁止ポリシーマップを要求する制限を記述するフィールドである。

【００４５】

ＣＲＬ参照ポイント（Certificate Revocation List Distribution Points）は、ユーザが公開鍵証明書を利用する際に、この公開鍵証明書が失効していないかどうかを確認するための失効リストの参照ポイントを記述するフィールドである。

【００４６】

署名は、公開鍵証明書発行者、すなわち、証明書発行認証局の署名フィールドである。電子署名は、公開鍵証明書の全体に対していわゆるハッシュ関数を適用してハッシュ値を生成し、このハッシュ値に対して証明書発行認証局の秘密鍵を用いて暗号化して生成したデータである。

【００４７】

証明書発行認証局は、このようなフォーマットからなる公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行ったユーザの排斥を行うための不正者リストの作成、管理、配布、すなわち、リボケーション（revocation）を行う。また、証明書発行認証局は、必要に応じて、公開鍵及び秘密鍵の生成も行う。

【００４８】

一方、この公開鍵証明書を利用するユーザは、自己が有する証明書発行認証局の公開鍵を用いて当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功すると、公開鍵証明書に基づいて公開鍵を取得し、この公開鍵を利用することができる。したがって、公開鍵証明書を利用する全てのユーザは、当該公開鍵証明書を発行した証明書発行認証局の公開鍵を有しているか取得する必要がある。

【００４９】

リモートアクセスシステムにおいては、後述するように、このような公開鍵証明書を各エンティティに保持させる。

【００５０】

つぎに、属性証明書について説明する。属性証明書は、証明書発行認証局とは異なるローカルな機関である属性認証局（Attribute Authority；ＡＡ）によって発行されるものである。

【００５１】

属性証明書は、図３及び図４に示すようなフォーマットから構成される。なお、同図においては、属性証明書を構成する各フィールド毎の項目と、これらの各項目に対する説明とを記載している。

【００５２】

図３に示すバージョン（version）は、属性証明書のフォーマットのバージョン情報を記述するフィールドであり、例えばフォーマットがバージョン２（１）である場合にはバージョン２（１）を示す”１”が記述される。

【００５３】

ホルダー（holder）は、属性証明書が結び付けられた公開鍵証明書の所有者を特定するためのフィールドである。ホルダーには、ベース認証局識別子（base Certificate ID）として、属性証明書の所有者が有する公開鍵証明書の発行者名（issuer）、属性証明書の所有者が有する公開鍵証明書のシリアルナンバ（serial）、属性証明書の所有者が有する公開鍵証明書の発行者を識別するための固有の識別子（issuer UID）が記述される。また、ホルダーには、公開鍵証明書におけるサブジェクト（subject）又はサブジェクト別名（subject Alt Name）と同一とされる属性証明書の所有者の名称（entity name）が記述される。さらに、ホルダーには、将来、属性証明書が識別情報（identity）や公開鍵証明書にリンクされていない場合を想定して、例えば公開鍵のハッシュが記述されるオブジェクト・ダイジェスト情報（object Digest Info）が記述される。

【００５４】

発行者（issuer）は、属性証明書に署名した発行者の情報を指定するフィールドである。

【００５５】

署名（signature）は、属性証明書の署名を有効にするために使用するアルゴリズムを識別するための識別子を記述するフィールドである。

【００５６】

シリアルナンバ（serial Number）は、属性認証局が各属性証明書に割り振るシリアルナンバを記述するフィールドである。

【００５７】

属性証明書有効期限（attr Cert Validity Period）は、属性証明書の有効期限である開始日時（not Before）及び終了日時（not After）を記述するフィールドである。

【００５８】

図４に示す属性（attributes）は、属性証明書の所有者の特権に関する情報を記述するフィールドであり、例えば、文章でアクセスが許可された対象物を記述してもよく、システム側で用意しておいたアクセスすることができるコードを記述してもよく、ある平文を暗号化する鍵を記述してもよい。例えば、属性には、属性証明書の検証者が当該属性証明書の所有者を認証する場合に利用するサービスに関する認証情報（Service Authentication Information）、属性証明書の検証者が用いる当該属性証明書の所有者のアクセス許可情報（Access Identity）、課金のために属性証明書の所有者を特定するための情報（Charging Identity）、属性証明書の所有者のグループへの帰属関係を示す情報（Group）、属性証明書の所有者に与えられる役割を示す情報（Role）、属性証明書の所有者に対する秘密情報の使用許可に関する情報（Clearance）が記述される。

【００５９】

発行者固有識別子（issuer Unique ID）は、属性証明書の発行者の公開鍵証明書で指定されている場合に利用されるフィールドである。

【００６０】

拡張情報（extensions）は、属性証明書の所有者の情報ではなく属性証明書の情報を記述するフィールドであり、サーバ及び／又はサービス管理者が属性証明書の所有者の監査を行い不正行為の検出、すなわち特定をするために用いる情報（Audit Identity）、属性証明書が対象とするサーバ及び／又はサービスを示す情報（AC Targeting）、属性証明書の検証者による当該属性証明書の署名確認の補助情報である属性証明書の発行者の鍵情報（Authority Key）、属性証明書の

検証者による当該属性証明書の失効状態確認の補助情報であるＯＣＳＰレスポンダのＵＲＩ（Uniform Resource Identifiers）を示す情報（Authority Information Access）、属性証明書の検証者による当該属性証明書の失効状態確認の補助情報であるＣＲＬ（Certificate Revocation List）配布点のＵＲＩを示す情報（CRL Distribution）、当該属性証明書に対応する失効情報がないことを示す情報（No Revocation）、提出者が所有者以外である場合に利用され、属性証明書を提出することができるエンティティを示す情報（Proxy Info）が記述される。

【００６１】

署名（signature Value）は、属性認証局によってつけられた署名を記述するフィールドである。

【００６２】

リモートアクセスシステムにおいては、後述するように、このようなフォーマットからなる属性証明書を各エンティティに保持させることにより、あるエンティティに対していかなる権限が許可されているのかを検証することができる。

【００６３】

リモートアクセスシステムは、以上のような公開鍵証明書及び属性証明書を用いて構築される。

【００６４】

以下、これらの公開鍵証明書及び属性証明書を用いたリモートアクセスシステムについて説明する。

【００６５】

まず、リモートアクセスシステムの概念について説明する。なお、ここでは、説明の便宜上、家庭内に設けられた各種情報家電又はパーソナルコンピュータ等の各種情報処理端末若しくはサーバ装置等をアクセスの対象とし、これらの機器に対して携帯電話機や携帯情報端末機（Personal Digital Assistants；ＰＤＡ）等の携帯機器を所持するユーザが屋外からアクセスするものとして説明する。

【００６６】

リモートアクセスシステムは、ＩＴＵ－Ｔ（International Telecommunication Union-Telecommunication sector）　Ｘ．５０９で定義されているＰＭＩ（Pr

ivilege management Infrastructure）の機能の１つである属性証明書を用いた権限プロキシ機能により、アクセスさせたいリソース毎に、権限単位での制御を行う。

【００６７】

ここで、権限プロキシ機能について図５を用いて説明する。

【００６８】

同図に示すように、属性証明書ＡＣを保持するクライアントＣＬと、このクライアントＣＬの権限を検証する権限検証側サーバＶＲとの間に、クライアントＣＬの権限を主張する権限主張側サーバＡＳが介在するシステムを考える。

【００６９】

この場合、クライアントＣＬは、権限検証側サーバＶＲに対してアクセスしようとする際には、権限主張側サーバＡＳに対して属性証明書ＡＣを提示し、これに応じて、権限主張側サーバＡＳは、クライアントＣＬから提示された属性証明書ＡＣを、権限検証側サーバＶＲに対して提示する。

【００７０】

しかしながら、この場合、権限検証側サーバＶＲは、権限主張側サーバＡＳから提示された属性証明書ＡＣが、権限主張側サーバＡＳの属性証明書ではないことから、アクセスを許可しない旨の検証結果を出すことになる。すなわち、このようなシステムにおいては、属性証明書を直接的に授受する装置間で、権限の主張及び検証が行われることから、クライアントＣＬが権限検証側サーバＶＲに対して自己の権限を主張しようとする際には、クライアントＣＬから権限検証側サーバＶＲに対して直接的に属性証明書ＡＣを提示する必要がある。

【００７１】

そこで、このようなシステムにおいては、先に図４に示した拡張情報（extensions）におけるプロシキ情報（Proxy Info）を利用する。このプロシキ情報は、上述したように、属性証明書の提出者が所有者以外である場合に利用され、属性証明書を提出することができるエンティティを示す情報である。

【００７２】

したがって、このようなシステムにおいては、クライアントＣＬは、権限検証

側サーバＶＲに対してアクセスしようとする際には、属性証明書を提出できるエンティティとして権限検証側サーバＶＲを含む旨を示すプロシキ情報を記述した属性証明書ＡＣを権限主張側サーバＡＳに対して提示し、これに応じて、権限主張側サーバＡＳは、クライアントＣＬから提示された属性証明書ＡＣを、権限検証側サーバＶＲに対して提示する。

【００７３】

これにより、権限検証側サーバＶＲは、権限主張側サーバＡＳから提示された属性証明書ＡＣにおけるプロシキ情報を参照して当該属性証明書ＡＣを検証し、アクセスを許可する旨の検証結果を出すことが可能となる。

【００７４】

このように、属性証明書ＡＣを保持するクライアントＣＬと、このクライアントＣＬの権限を検証する権限検証側サーバＶＲとの間に、クライアントＣＬの権限を主張する権限主張側サーバＡＳが介在するシステムにおいては、プロシキ情報に属性証明書ＡＣの提出先を記述することにより、クライアントＣＬが権限検証側サーバＶＲに対してアクセスすることが可能となる。

【００７５】

リモートアクセスシステムは、このような権限プロキシ機能を利用する。概念的には、リモートアクセスシステムは、図６に示すように、上述した公開鍵証明書を発行する証明書発行認証局ＣＡと、上述した属性証明書を発行する属性認証局ＡＡと、アクセスの対象となる対象機器10_1，10_2と、これらの対象機器10_1，10_2が属する家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースであるホームゲートウェイと２０と、対象機器10_1，10_2に対してアクセスするためにユーザが所持する携帯機器３０とを、エンティティとして備える。

【００７６】

証明書発行認証局ＣＡは、公開鍵暗号方式における独立した所定の第三者機関であって、ＩＳＯ／ＩＥＣ　９５９４－８、又はＩＴＵ－Ｔ　Ｘ．５０９に基づく電子証明書である公開鍵証明書を発行する。具体的には、証明書発行認証局ＣＡは、公開鍵証明書PKC_{T1}，PKC_{T2}を、それぞれ、対象機器10_1，１

０_2に対して発行するとともに、公開鍵証明書$ＰＫＣ_G$をホームゲートウェイ２０に対して発行するとともに、公開鍵証明書$ＰＫＣ_M$を携帯機器３０に対して発行する。なお、この公開鍵証明書の発行の形態は、様々なものが考えられるが、例えば、対象機器１０_1，１０_2、ホームゲートウェイ２０、及び携帯機器３０の製造時にデータとして埋め込むことが考えられる。

【００７７】

属性認証局ＡＡは、証明書発行認証局ＣＡとは論理的に異なるローカルな機関であって、権限管理を行うために用いる電子証明書である属性証明書を発行する。属性認証局ＡＡは、証明書発行認証局ＣＡからホームゲートウェイ２０に対して発行された公開鍵証明書$ＰＫＣ_G$により、ホームゲートウェイ２０の認証を行う。そして、属性認証局ＡＡは、例えばホームゲートウェイ２０がユーザサイドに渡ってから初回接続時等に、携帯機器３０に対して属性証明書$ＡＣ_P$を発行する許可を与えるための属性証明書$ＡＣ_L$を、ホームゲートウェイ２０に対して発行する。なお、この属性証明書$ＡＣ_L$については、後に詳述するものとする。

【００７８】

対象機器１０_1，１０_2は、それぞれ、図５における権限検証側サーバＶＲに相当するものである。対象機器１０_1，１０_2は、それぞれ、例えば、ネットワークに接続可能な各種情報家電や、パーソナルコンピュータ等の各種情報処理端末若しくはホームサーバ等のサーバ装置を想定したものであり、家庭内ネットワークを構成する機器である。なお、本発明におけるリソースとは、後に具体的な適用例を述べるように、ログインするこれらの対象機器１０_1，１０_2そのものを示す場合がある他、これらの対象機器１０_1，１０_2が保持するファイル等のデータやその他の各種情報を含む概念であるが、ここでは説明の便宜上、対象機器１０_1，１０_2そのものをリソースとするものとして説明する。対象機器１０_1，１０_2は、それぞれ、証明書発行認証局ＣＡによって発行された公開鍵証明書$ＰＫＣ_{T1}$，$ＰＫＣ_{T2}$を保持し、これらの公開鍵証明書$ＰＫＣ_{T1}$，$ＰＫＣ_{T2}$を用いてホームゲートウェイ２０との間で相互認証を行う。また、対象機器１０_1，１０_2は、それぞれ、携帯機器３０がアクセスする際に送信した属性証明書$ＡＣ_P$をホームゲートウェイ２０を介して受信し、この属性証明書$ＡＣ_P$の

検証を行う。

【００７９】

ホームゲートウェイ２０は、図５における権限主張側サーバＡＳに相当するものである。ホームゲートウェイ２０は、例えば、いわゆるホームルータ、ファイアウォール、及び／又はブリッジといった概念を含むものであり、異なるプロトコルのネットワーク同士の接続を可能とするネットワークの入り口に相当する機器であり、対象機器10_1，10_2が属する家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能する。ホームゲートウェイ２０は、証明書発行認証局ＣＡによって発行された公開鍵証明書PKC_Gを保持し、この公開鍵証明書PKC_Gを用いて対象機器10_1，10_2、携帯機器３０、及び属性認証局ＡＡとの間で相互認証を行う。また、ホームゲートウェイ２０は、携帯機器３０に対して属性証明書AC_Pを発行する許可を与えるための属性証明書AC_Lが属性認証局ＡＡによって発行されると、この属性証明書AC_Lを保持し、この属性証明書AC_Lに基づいて、携帯機器３０に対して属性証明書AC_Pを発行する。なお、この属性証明書AC_Pについては、後に詳述するものとする。さらに、ホームゲートウェイ２０は、携帯機器３０から送信された属性証明書AC_Pを受信すると、この属性証明書AC_Pを対象機器10_1，10_2のそれぞれに対して送信して提示する。

【００８０】

携帯機器３０は、図５におけるクライアントＣＬに相当するものである。携帯機器３０は、屋外にいるユーザが所持する携帯電話機や携帯情報端末機等の機器であり、いわゆるインターネット等のセキュアでないネットワークＮＴを介してホームゲートウェイ２０に対して接続可能とされる。携帯機器３０は、証明書発行認証局ＣＡによって発行された公開鍵証明書PKC_Mを保持し、この公開鍵証明書PKC_Mを用いてホームゲートウェイ２０との間で相互認証を行う。また、携帯機器３０は、リソースとしての対象機器10_1，10_2のそれぞれに対してアクセスすることを認証するための属性証明書AC_Pがホームゲートウェイ２０によって発行されると、この属性証明書AC_PをＩＣ（Integrated Circuit）カード等に格納すること等によって保持する。そして、携帯機器３０は、対象機器

１０$_1$，１０$_2$のそれぞれに対してアクセスしようと試みる際に、ＩＣカード等に格納された属性証明書ＡＣ$_P$を用いたログイン操作を行うことにより、この属性証明書ＡＣ$_P$をホームゲートウェイ２０に対して送信して提示する。

【００８１】

このようなリモートアクセスシステムにおいては、上述したように、２つの属性証明書ＡＣ$_L$，ＡＣ$_P$が使用される。

【００８２】

まず、属性証明書ＡＣ$_L$について説明する。

【００８３】

属性証明書ＡＣ$_L$は、上述したように、携帯機器３０に対して属性証明書ＡＣ$_P$を発行する許可をホームゲートウェイ２０に対して与えるために、属性認証局ＡＡからホームゲートウェイ２０に対して発行されるものである。例えば、この属性証明書ＡＣ$_L$には、図７にタイプとして登録されているオブジェクトＩＤ（Object ID；ＯＩＤ）及び値の例の抜粋を示す先に図４に示した属性（attributes）における各フィールドのうち、当該属性証明書ＡＣ$_L$の所有者たるホームゲートウェイ２０に与えられる役割を示す情報（Role）を用いて、携帯機器３０に対して属性証明書ＡＣ$_P$を発行する許可を与える旨を示す情報を記述することができる。

【００８４】

ここで、”ロール（Role）”の概念について説明する。

【００８５】

この”ロール（Role）”の概念を用いた権限管理の手法は、本件出願人が先に出願している特願２００２－０２９６３６に記載したものである。

【００８６】

すなわち、この権限管理の手法においては、概念的には、図８に示すように、例えば権限ＡＵ$_{11}$，ＡＵ$_{12}$，・・・，ＡＵ$_{21}$，ＡＵ$_{22}$，・・・といった所定の権限を定義する枠組みを１つの役割（ロール）Ｒ$_1$，Ｒ$_2$とし、例えば個人Ｍ$_1$，Ｍ$_2$，Ｍ$_3$といった少なくとも１人以上の個人がこのロールＲ$_1$，Ｒ$_2$に属するものとされる。

【００８７】

この権限管理の手法においては、各個人M_1，M_2，M_3がそれぞれ有する属性証明書であって当該個人M_1，M_2，M_3が属しているロールを示す情報が記述されている役割割当証明書（Role Assignment Certificate）ＲＡＡＣが、属性認証局ＡＡによって発行されるとともに、ロール毎に発行される属性証明書であって当該ロールに許可されている権限を示す情報が記述されている役割定義証明書（Role Specification Certificate）ＲＳＡＣが、役割認証局（Role Authority）ＲＡによって発行される。なお、役割認証局ＲＡは、属性認証局ＡＡと同一であってもよいが、ここでは説明の便宜上、論理的に独立な機関であるものとする。

【００８８】

この権限管理の手法においては、各ロールの定義については、役割認証局ＲＡによって発行される役割定義証明書ＲＳＡＣを用いる。すなわち、この権限管理の手法においては、ロール毎に、許可される手続きが定義されるが、この情報が、役割認証局ＲＡによって発行される役割定義証明書ＲＳＡＣに記述される。

【００８９】

この役割定義証明書ＲＳＡＣは、先に図３及び図４に示した属性証明書のフォーマットにしたがって作成されるものであり、少なくとも、当該役割定義証明書ＲＳＡＣの発行者たる役割認証局ＲＡの名前を示す情報、ロールを識別するためのロール名といったロールの情報、システムによってコード又は操作名が記述されるものであって許可される操作を示す情報等の各種情報が記述される。

【００９０】

リモートアクセスシステムにおいては、携帯機器３０に対して属性証明書AC_Pを発行する許可を与える旨を示す情報を含む各種情報が記述された役割定義証明書ＲＳＡＣが役割認証局ＲＡによって発行され、権限AU_{11}，AU_{12}，・・・，AU_{21}，AU_{22}，・・・が定義されたリソース、すなわち、先に示した図６においては対象機器10_1，10_2がこの役割定義証明書ＲＳＡＣを保持する。

【００９１】

一方、この権限管理の手法においては、各ロールに対する役割の割り当てについては、属性認証局ＡＡによって発行される役割割当証明書ＲＡＡＣを用いる。すなわち、この権限管理の手法においては、個人M_1，M_2，M_3毎に、各役割が定義されるが、この情報が、属性認証局ＡＡによって発行される役割割当証明書ＲＡＡＣに記述される。

【００９２】

この役割割当証明書ＲＡＡＣも、役割定義証明書ＲＳＡＣと同様に、先に図３及び図４に示した属性証明書のフォーマットにしたがって作成されるものであり、少なくとも、当該役割割当証明書ＲＡＡＣの発行者たる属性認証局ＡＡの名前を示す情報、ロールを識別するためのロール名といったロールの情報、対応する役割定義証明書ＲＳＡＣと関連付けを行うための役割定義証明書ＲＳＡＣへの参照ポイントを示す情報としての役割認証局ＲＡの名前を示す情報等の各種情報が記述される。

【００９３】

リモートアクセスシステムにおいては、このような各種情報が記述された役割割当証明書ＲＡＡＣが属性証明書AC_Lとして属性認証局ＡＡによって発行され、個人M_1，M_2，M_3、すなわち、先に示した図６においてはホームゲートウェイ２０が、この役割割当証明書ＲＡＡＣを保持する。

【００９４】

リモートアクセスシステムにおいては、このような”ロール（Role）”の概念を用いることにより、携帯機器３０に対して属性証明書AC_Pを発行する許可を与える旨を示す情報を記述した属性証明書AC_Lを、属性認証局ＡＡによってホームゲートウェイ２０に対して発行することができる。これにより、リモートアクセスシステムにおいては、この属性証明書AC_Lを保持したホームゲートウェイ２０によって属性証明書AC_Pを携帯機器３０に対して発行することが可能となる。

【００９５】

なお、リモートアクセスシステムにおいては、携帯機器３０に対して属性証明書AC_Pを発行する許可を与える旨を示す情報を属性証明書AC_Lに記述するた

めに、当該属性証明書$ＡＣ_{L}$の所有者たるホームゲートウェイ２０に与えられる役割を示す情報（Role）を用いるのではなく、図７に示した属性（attributes）における各フィールドのうち、属性証明書の検証者が当該属性証明書の所有者を認証する場合に利用するサービスに関する認証情報（Service Authentication Information）や、属性証明書の検証者が用いる当該属性証明書の所有者のアクセス許可情報（Access Identity）等を用いて、同情報を記述することも可能である。

【００９６】

また、リモートアクセスシステムにおいては、権限委譲エクステンションを用い、属性証明書$ＡＣ_{P}$を発行する対象及び権限を制御するようにしてもよい。例えば、リモートアクセスシステムにおいては、Basic Attribute Constraintsエクステンションを用いて、ホームゲートウェイ２０には携帯機器３０に対して属性証明書$ＡＣ_{P}$を発行できる旨を示し、さらに、ホームゲートウェイ２０からは権限委譲を許可しない旨を設定することが考えられる。

【００９７】

このように、リモートアクセスシステムにおいては、携帯機器３０に対して属性証明書$ＡＣ_{P}$を発行する許可をホームゲートウェイ２０に与える手法として、様々なものが考えられる。

【００９８】

つぎに、属性証明書$ＡＣ_{P}$について説明する。

【００９９】

属性証明書$ＡＣ_{P}$は、ある公開鍵証明書を保持している機器又はユーザに対する権限が記述されたものであり、ここでは、公開鍵証明書$ＰＫＣ_{M}$を保持している携帯機器３０に対する権限として、リソースとしての対象機器１０_{1}，１０_{2}のそれぞれに対してアクセスすることを許可する旨の情報が記述されたものである。例えば、この属性証明書$ＡＣ_{P}$には、先に図７に示した属性（attributes）における各フィールドのうち、属性証明書$ＡＣ_{P}$の検証者たる対象機器１０_{1}，１０_{2}のそれぞれが当該属性証明書$ＡＣ_{P}$の所有者を認証する場合に利用するサービスに関する認証情報（Service Authentication Information）や、属性証明

書$ＡＣ_{P}$の検証者たる対象機器１０_{1}，１０_{2}のそれぞれが用いる当該属性証明書$ＡＣ_{P}$の所有者のアクセス許可情報（Access Identity）等を用いて、アクセスする対象、アクセスできる操作（権限）、及びアクセスするための認証情報がある場合には当該認証情報を記述することができる。また、属性証明書$ＡＣ_{P}$には、図９にタイプとして登録されているオブジェクトＩＤ（Object ID；ＯＩＤ）及びクリティカル又は値の例の抜粋を示す先に図４に示した拡張情報（extensions）における各フィールドのうち、プロシキ情報（Proxy Info）を用いて、当該属性証明書$ＡＣ_{P}$を経由させるホームゲートウェイ２０の情報が記述される。

【０１００】

ここで、プロシキ情報は、具体的には、図１０に示すように記述されるものである。

【０１０１】

属性証明書$ＡＣ_{P}$には、このようなプロシキ情報におけるターゲット（Target）として、ホームゲートウェイ２０を識別するためのアドレスや識別子が記述されるとともに、ホームゲートウェイ２０が保持する公開鍵証明書$ＰＫＣ_{G}$を示す情報が記述される。

【０１０２】

このように、リモートアクセスシステムにおいては、携帯機器３０に対する権限として、リソースとしての対象機器１０_{1}，１０_{2}のそれぞれに対してアクセスすることを許可する旨の情報が記述されるとともに、プロシキ情報として、ホームゲートウェイ２０の情報が記述された属性証明書$ＡＣ_{P}$を、ホームゲートウェイ２０から携帯機器３０に対して発行することができる。これにより、リモートアクセスシステムにおいては、対象機器１０_{1}，１０_{2}が、それぞれ、この属性証明書$ＡＣ_{P}$をホームゲートウェイ２０を介して受信した場合には、プロシキ情報におけるターゲットを検証し、且つ、ホームゲートウェイ２０から送信された属性証明書であることを検証することになる。

【０１０３】

さて、このようなリモートアクセスシステムにおいては、具体的には、図１１に示すように、当該リモートアクセスシステムを構築するための準備フェーズＰ

１が行われると、任意の携帯機器をリソースに対してアクセスする機器として登録するための登録フェーズＰ２が行われる。これにより、リモートアクセスシステムにおいては、登録された携帯機器が任意の操作を行うことが可能となり、実際に携帯機器が任意の操作を行う際には、アクセスフェーズＰ３が行われる。また、リモートアクセスシステムにおいては、必要に応じて、任意の携帯機器をリソースに対してアクセスする機器から除外するためのアクセス削除フェーズＰ４や、任意の携帯機器の権限を変更するためのアクセス変更フェーズＰ５が行われる。

【０１０４】

以下、これら５つの各フェーズについて説明する。

【０１０５】

まず、準備フェーズＰ１について説明する。

【０１０６】

リモートアクセスシステムにおいては、当該リモートアクセスシステムを構築するための準備フェーズＰ１として、各エンティティが相互認証可能となるように、証明書発行認証局ＣＡにより、各エンティティに対して認証のための公開鍵証明書を発行する。すなわち、リモートアクセスシステムにおいては、上述したように、各エンティティの製造時等に、証明書発行認証局ＣＡにより、公開鍵証明書PKC_{T1}，PKC_{T2}を、それぞれ、対象機器10_1，10_2に対して発行するとともに、公開鍵証明書PKC_Gをホームゲートウェイ２０に対して発行するとともに、公開鍵証明書PKC_Mを携帯機器３０に対して発行する。

【０１０７】

リモートアクセスシステムは、このような準備フェーズＰ１を経ることにより、各エンティティが相互認証可能な状態に構築される。

【０１０８】

つぎに、登録フェーズＰ２について説明する。

【０１０９】

リモートアクセスシステムにおいては、任意の携帯機器としての携帯機器３０をリソースに対してアクセスする機器として登録するための登録フェーズＰ２と

して、図１２に示す工程が行われる。

【０１１０】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ１において、属性認証局ＡＡにより、上述した準備フェーズＰ１にて証明書発行認証局ＣＡによって発行されてホームゲートウェイ２０に保持されている公開鍵証明書PKC_Gを用いて、ホームゲートウェイ２０との間で相互認証を行う。この相互認証は、ホームゲートウェイ２０自体に対する認証であり、ホームゲートウェイ２０が正当なものであるか否かを認証するためのものである。

【０１１１】

続いて、リモートアクセスシステムにおいては、ステップＳ２において、属性認証局ＡＡにより、ホームゲートウェイ２０がユーザサイドに渡ってから初回接続時等に、携帯機器３０に対して属性証明書AC_Pを発行する許可を与えるための属性証明書AC_Lを、ホームゲートウェイ２０に対して発行する。これにともない、ホームゲートウェイ２０は、属性認証局ＡＡから送信された属性証明書AC_Lを保持する。

【０１１２】

続いて、リモートアクセスシステムにおいては、ステップＳ３において、ホームゲートウェイ２０により、ユーザからの指示にしたがい、接続する機器、すなわち、対象機器10_1，10_2のそれぞれの情報を登録するとともに、その対象機器10_1，10_2のそれぞれに対してリモートからアクセスしてもよい携帯機器３０に対して上述したプロシキ情報を記述した属性証明書AC_Pを発行する。

【０１１３】

続いて、リモートアクセスシステムにおいては、ステップＳ４において、携帯機器３０により、上述した準備フェーズＰ１にて証明書発行認証局ＣＡによって発行されて保持している公開鍵証明書PKC_Mを用いて、ホームゲートウェイ２０との間で相互認証を行う。

【０１１４】

そして、リモートアクセスシステムにおいては、ステップＳ５において、携帯機器３０により、ホームゲートウェイ２０から送信された属性証明書AC_PをＩ

Ｃカード等に格納して保持し、一連の登録フェーズＰ２を終了する。

【０１１５】

リモートアクセスシステムにおいては、このような一連の工程からなる登録フェーズＰ２を経ることにより、リソースに対してアクセスする機器として、携帯機器３０を登録することができる。このようにしてリソースに対してアクセスする携帯機器３０の登録がされたリモートアクセスシステムにおいては、登録された携帯機器３０が任意の操作を行うことが可能となる。

【０１１６】

つぎに、アクセスフェーズＰ３について説明する。

【０１１７】

リモートアクセスシステムにおいては、登録された携帯機器３０がリソースに対してアクセスする際には、アクセスフェーズＰ３として、図１３に示す工程が行われる。

【０１１８】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ１１において、携帯機器３０により、保持している公開鍵証明書PKC_Mを用いて、ホームゲートウェイ２０との間で相互認証を行う。

【０１１９】

続いて、リモートアクセスシステムにおいては、ステップＳ１２において、携帯機器３０により、保持している属性証明書AC_Pをホームゲートウェイ２０に対して送信して提示する。

【０１２０】

これに応じて、リモートアクセスシステムにおいては、ステップＳ１３において、ホームゲートウェイ２０により、携帯機器３０から提示された属性証明書AC_Pの内容に基づいて、当該属性証明書AC_Pを、アクセスする対象として指定された機器、すなわち、対象機器10_1，10_2のいずれか又は双方に対して送信して提示する。

【０１２１】

続いて、リモートアクセスシステムにおいては、ステップＳ１４において、対

象機器１０$_1$，１０$_2$のいずれか又は双方により、ホームゲートウェイ２０から送信された属性証明書ＡＣ$_P$を受信し、上述したプロシキ情報や属性といった当該属性証明書ＡＣ$_P$の内容を検証する。

【０１２２】

リモートアクセスシステムにおいては、ステップＳ１５において、属性証明書ＡＣ$_P$の検証結果が正当なものであった場合には、ステップＳ１６において、対象機器１０$_1$，１０$_2$のいずれか又は双方によって携帯機器３０のアクセスを許可し、一連のアクセスフェーズＰ３を終了する。一方、リモートアクセスシステムにおいては、ステップＳ１５において、属性証明書ＡＣ$_P$の検証結果が不当なものであった場合には、ステップＳ１７において、対象機器１０$_1$，１０$_2$のいずれか又は双方によって携帯機器３０のアクセスを拒否し、一連のアクセスフェーズＰ３を終了する。

【０１２３】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセスフェーズＰ３を経ることにより、対象機器１０$_1$，１０$_2$のそれぞれによって携帯機器３０の権限を判別することができ、アクセスが許可された携帯機器３０は、任意の操作を行うことが可能となる。

【０１２４】

つぎに、アクセス削除フェーズＰ４について説明する。

【０１２５】

リモートアクセスシステムにおいては、任意の携帯機器をリソースに対してアクセスする機器から除外したい場合には、アクセス削除フェーズＰ４として、図１４に示す工程が行われる。

【０１２６】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ２１において、ホームゲートウェイ２０により、ユーザからの指示にしたがい、対象機器１０$_1$，１０$_2$のそれぞれに対してリモートからアクセスしてもよい携帯機器３０に対して発行した属性証明書ＡＣ$_P$に対するＣＲＬ（ＡＣＲＬ）を作成し、このＣＲＬ（ＡＣＲＬ）を保持する。

【０１２７】

このように、リモートアクセスシステムにおいては、属性証明書$ＡＣ_{P}$に対するＣＲＬ（ＡＣＲＬ）を作成することにより、携帯機器３０からホームゲートウェイ２０に対してアクセスがあった場合には、ホームゲートウェイ２０によってアクセスを拒否することができ、携帯機器３０をリソースに対してアクセスする機器から除外することができる。特に、リモートアクセスシステムは、複数人のユーザの間で携帯機器３０の貸借がある場合や携帯機器３０を紛失した場合といった携帯機器３０の側の都合による場合等には、属性証明書$ＡＣ_{P}$に対するＣＲＬ（ＡＣＲＬ）を作成するのみで、携帯機器３０をリソースに対してアクセスする機器から除外することができる。

【０１２８】

ただし、リモートアクセスシステムにおいては、このような操作を繰り返し行うことにより、ＣＲＬ（ＡＣＲＬ）のサイズが大きくなり、取り扱いに不便を生じるおそれがある。

【０１２９】

そこで、リモートアクセスシステムにおいては、正当なユーザが自らの意思で携帯機器３０をリソースに対してアクセスする機器から除外したい場合等には、ステップＳ２１の処理に続いて、以下のステップＳ２２乃至ステップＳ２４の処理を行うようにしてもよい。

【０１３０】

すなわち、リモートアクセスシステムにおいては、ステップＳ２２において、携帯機器３０により、保持している公開鍵証明書$ＰＫＣ_{M}$を用いて、ホームゲートウェイ２０との間で相互認証を行う。

【０１３１】

続いて、リモートアクセスシステムにおいては、ステップＳ２３において、ホームゲートウェイ２０からの指示にしたがい、携帯機器３０により、保持している属性証明書$ＡＣ_{P}$を削除する。

【０１３２】

そして、リモートアクセスシステムにおいては、ステップＳ２４において、ホ

ームゲートウェイ２０により、ステップＳ２１にて作成したＣＲＬ（ＡＣＲＬ）を削除し、一連のアクセス削除フェーズＰ４を終了する。

【０１３３】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス削除フェーズＰ４を経ることにより、携帯機器３０をリソースに対してアクセスする機器から除外することができる。

【０１３４】

最後に、アクセス変更フェーズＰ５について説明する。

【０１３５】

リモートアクセスシステムにおいては、任意の携帯機器の権限を変更したい場合には、アクセス変更フェーズＰ５として、図１５に示す工程が行われる。

【０１３６】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ３１において、ホームゲートウェイ２０により、ユーザからの指示にしたがい、携帯機器３０に対してプロシキ情報を記述した新たな属性証明書$ＡＣ_{P}$を発行する。

【０１３７】

続いて、リモートアクセスシステムにおいては、ステップＳ３２において、携帯機器３０により、保持している公開鍵証明書$ＰＫＣ_{M}$を用いて、ホームゲートウェイ２０との間で相互認証を行う。

【０１３８】

そして、リモートアクセスシステムにおいては、ステップＳ３３において、携帯機器３０により、ホームゲートウェイ２０から送信された新たな属性証明書$ＡＣ_{P}$を、元の属性証明書$ＡＣ_{P}$と置換してＩＣカード等に格納して保持し、一連のアクセス変更フェーズＰ５を終了する。

【０１３９】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス変更フェーズＰ５を経ることにより、携帯機器３０の権限を変更することができる。これにより、リモートアクセスシステムにおいては、携帯機器３０が新た

な任意の操作を行うことが可能となる。

【０１４０】

以上のように、リモートアクセスシステムは、プロシキ情報が記述された属性証明書$ＡＣ_{P}$を用いて権限管理を行うことができる。

【０１４１】

さて、以下では、このようなリモートアクセスシステムを具体的に適用した適用例について説明する。なお、本発明におけるリソースとは、上述したように、ログインする機器そのものを示す場合がある他、これらの機器が保持するファイル等のデータやその他の各種情報を含む概念であるが、ここでは、これらリソースの具体例についても言及する。

【０１４２】

まず、リモートアクセスシステムの適用例としては、ホームサーバやパーソナルコンピュータ等の情報処理端末が保持するデータへのリモートアクセスを行うデータアクセスシステムがあげられる。

【０１４３】

このデータアクセスシステムにおいては、ホームサーバや情報処理端末が保持するデータがリソースとなり、携帯機器を用いてユーザが行う操作は、データを保持するホームサーバや情報処理端末に対するデータアクセスとなる。

【０１４４】

このようなデータアクセスシステムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書$ＡＣ_{P}$を携帯機器に対して発行し、携帯機器がデータにアクセスする際に、当該属性証明書$ＡＣ_{P}$をホームゲートウェイを介してホームサーバや情報処理端末に対して提示する。これにより、データアクセスシステムにおいては、携帯機器を用いてホームゲートウェイを介してデータに対してアクセスすることが可能となる。

【０１４５】

このように、リモートアクセスシステムは、ホームサーバやパーソナルコンピュータ等の情報処理端末が保持するデータに対するデータアクセスシステムに適用することができる。

【０１４６】

また、リモートアクセスシステムの他の適用例としては、家電カメラを用いた画像撮影による情報取得システムがあげられる。

【０１４７】

具体的に説明するために、例えば家庭内の冷蔵庫の在庫を情報として取得する情報取得システムを考える。この情報取得システムにおいては、冷蔵庫内部の画像がリソースとなり、携帯機器を用いてユーザが行う操作は、取得した画像を閲覧することによる冷蔵庫の在庫確認となる。

【０１４８】

このような情報取得システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書ACpを携帯機器に対して発行し、携帯機器が家電カメラが内部に取り付けられた冷蔵庫にアクセスする際に、当該属性証明書ACpをホームゲートウェイを介して冷蔵庫に対して提示する。これにより、情報取得システムにおいては、ユーザが外出している最中であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介して家電カメラを操作し、冷蔵庫内部の画像を取得することが可能となる。

【０１４９】

このように、リモートアクセスシステムは、家電カメラを用いた画像撮影による情報取得システムに適用することができる。

【０１５０】

さらに、リモートアクセスシステムの他の適用例としては、任意の場所の画像撮影による情報取得システムがあげられる。

【０１５１】

具体的に説明するために、例えば所定の会員である旨を証明するための会員カードの画像を取得することによって会員であるか否かを認証する情報取得システムを考える。この情報取得システムにおいては、家庭等の任意の場所にある会員カードの画像がリソースとなり、携帯機器を用いてユーザが行う操作は、会員カードの認証者に画像を閲覧させることによって会員である旨を証明するものとなる。

【０１５２】

このような情報取得システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書$ＡＣ_{P}$を携帯機器に対して発行し、携帯機器が会員カードを撮影するカメラにアクセスする際に、当該属性証明書$ＡＣ_{P}$をホームゲートウェイを介してカメラに対して提示する。これにより、情報取得システムにおいては、会員カードがユーザの手元にない場合であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介してカメラを操作し、会員カードの画像を取得することが可能となる。

【０１５３】

このように、リモートアクセスシステムは、任意の場所の画像撮影による情報取得システムに適用することができる。

【０１５４】

さらにまた、リモートアクセスシステムの他の適用例としては、屋外からのリモート操作による家電操作を行う家電操作システムがあげられる。

【０１５５】

具体的に説明するために、例えば家庭内のエアーコンディショナ機器のオン／オフ操作を行う家電操作システムを考える。この家電操作システムにおいては、エアーコンディショナ機器自体がリソースとなり、携帯機器を用いてユーザが行う操作は、このリソースとしてのエアーコンディショナ機器をリモート操作するためのリモートコントローラに対するアクセスとなる。

【０１５６】

このような家電操作システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書$ＡＣ_{P}$を携帯機器に対して発行し、携帯機器がリモートコントローラにアクセスする際に、当該属性証明書$ＡＣ_{P}$をホームゲートウェイを介してリモートコントローラに対して提示する。これにより、家電操作システムにおいては、ユーザが外出している最中であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介してリモートコントローラを操作し、エアーコンディショナ機器のオン／オフ操作を行うことが可能となる。

【０１５７】

このように、リモートアクセスシステムは、屋外からのリモート操作による家電操作を行う家電操作システムに適用することができる。

【０１５８】

以上説明したように、本発明の実施の形態として示したリモートアクセスシステムは、プロシキ情報が記述された属性証明書AC_Pを用いて権限管理を行うことにより、携帯機器３０からリソースとしての対象機器10_1，10_2のそれぞれに対してリモートアクセスを行う際に、対象機器10_1，10_2毎に、権限単位での制御を容易に行うことができる。

【０１５９】

また、このリモートアクセスシステムは、属性証明書AC_Pを利用する際に、リソースとしての対象機器10_1，10_2のそれぞれが属するネットワークの入り口となるホームゲートウェイ２０を経由して、対象機器10_1，10_2のそれぞれと携帯機器３０との間で属性証明書AC_Pの授受を行うことにより、属性証明書AC_Pの送付ルートが一義に決定されることから、属性証明書AC_Pの送付ルートを確認することができ、セキュリティを向上させることができる。

【０１６０】

なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、アクセスの対象となる対象機器10_1，10_2が属する家庭内ネットワークの入り口となるホームゲートウェイ２０が携帯機器３０に対して属性証明書AC_Pを発行するものとして説明したが、本発明は、属性証明書AC_Pを発行するエンティティに拘泥するものではなく、ホームゲートウェイ２０は、少なくとも属性証明書AC_Pの内容に応じて、当該属性証明書AC_Pを適切な提示先に提示する機能を有するものであればよい。

【０１６１】

この具体例として、あるネットワークの入り口としてのホームゲートウェイによって発行された属性証明書AC_Pを用いて、他のネットワークに属するリソースにアクセスするリモートアクセスシステムについて説明する。

【０１６２】

このリモートアクセスシステムは、概念的には、図１６に示すように、第１の

家庭内ネットワークに属する対象機器１０$_1$，１０$_2$と、これらの対象機器１０$_1$，１０$_2$が属する第１の家庭内ネットワークの入り口となるホームゲートウェイと２０$_1$と、対象機器１０$_1$，１０$_2$に対してアクセスするためにユーザが所持する携帯機器３０$_1$と、第１の家庭内ネットワークとは異なる第２の家庭内ネットワークに属する対象機器１０$_3$と、この対象機器１０$_3$が属する第２の家庭内ネットワークの入り口となるホームゲートウェイと２０$_2$と、対象機器１０$_3$に対してアクセスするために他のユーザが所持する携帯機器３０$_2$と、図示しないが、上述した証明書発行認証局ＣＡ及び属性認証局ＡＡとを、エンティティとして備える。

【０１６３】

すなわち、このリモートアクセスシステムは、第１の家庭内ネットワークから構成される図６に示したようなシステムと、他の家屋等の第２のネットワークから構成される同様のシステムとが、併存しているものである。

【０１６４】

対象機器１０$_1$，１０$_2$は、それぞれ、第１の家庭内ネットワークを構成する機器であり、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書ＰＫＣ$_{T1}$，ＰＫＣ$_{T2}$を保持し、これらの公開鍵証明書ＰＫＣ$_{T1}$，ＰＫＣ$_{T2}$を用いてホームゲートウェイ２０$_1$との間で相互認証を行う。また、対象機器１０$_1$，１０$_2$は、それぞれ、携帯機器３０$_1$がアクセスする際に送信した属性証明書ＡＣ$_{P1}$をホームゲートウェイ２０$_1$を介して受信し、この属性証明書ＡＣ$_{P1}$の検証を行う。

【０１６５】

ホームゲートウェイ２０$_1$は、対象機器１０$_1$，１０$_2$が属する第１の家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能する。ホームゲートウェイ２０$_1$は、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書ＰＫＣ$_{G1}$を保持し、この公開鍵証明書ＰＫＣ$_{G1}$を用いて対象機器１０$_1$，１０$_2$、携帯機器３０$_1$、及び図示しない属性認証局ＡＡとの間で相互認証を行う。また、ホームゲートウェイ２０$_1$は、携帯機器３０$_1$に対して属性証明書ＡＣ$_{P1}$を発行する許可を与えるための属性証明書

ACL_1が図示しない属性認証局ＡＡによって発行されると、この属性証明書ACL_1を保持し、この属性証明書ACL_1に基づいて、携帯機器30_1に対して属性証明書ACP_1を発行する。さらに、ホームゲートウェイ20_1は、携帯機器30_1から送信された属性証明書ACP_1を受信すると、この属性証明書ACP_1を対象機器10_1，10_2のそれぞれに対して送信して提示する。

【０１６６】

さらにまた、ホームゲートウェイ20_1は、アクセスすることができる他のネットワークにおけるホームゲートウェイを示す情報が記述された後に詳述する属性証明書ACHが図示しない属性認証局ＡＡによって発行されると、この属性証明書ACHを保持し、この属性証明書ACHに基づいて、第２の家庭内ネットワークにおけるホームゲートウェイ20_2と通信を行うことが可能とされる。ホームゲートウェイ20_1は、この属性証明書ACHを第２の家庭内ネットワークにおけるホームゲートウェイ20_2に対して送信して提示することにより、第２の家庭内ネットワークに属する対象機器10_3に対するアクセス許可を得るための属性証明書ACP_1'をホームゲートウェイ20_2によって発行してもらい、携帯機器30_1に対してこの属性証明書ACP_1'を送信する。そして、ホームゲートウェイ20_1は、携帯機器30_1から送信された属性証明書ACP_1'を受信すると、この属性証明書ACP_1'を属性証明書ACHとともにホームゲートウェイ20_2に対して送信して提示する。なお、この属性証明書ACP_1'については、後に詳述するものとする。

【０１６７】

携帯機器30_1は、通常は、第１の家庭内ネットワークに属する対象機器10_1，10_2のそれぞれに対してアクセスするための機器であり、インターネット等のセキュアでないネットワークＮＴを介してホームゲートウェイ20_1に対して接続可能とされる。携帯機器30_1は、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書PKC_{M1}を保持し、この公開鍵証明書PKC_{M1}を用いてホームゲートウェイ20_1との間で相互認証を行う。携帯機器30_1は、リソースとしての対象機器10_1，10_2のそれぞれに対してアクセスすることを認証するための属性証明書ACP_1がホームゲートウェイ20_1によって発

行されると、この属性証明書ACP_1をＩＣカード等に格納すること等によって保持する。そして、携帯機器30_1は、対象機器10_1，10_2のそれぞれに対してアクセスしようと試みる際に、ＩＣカード等に格納された属性証明書ACP_1を用いたログイン操作を行うことにより、この属性証明書ACP_1をホームゲートウェイ20_1に対して送信して提示する。

【０１６８】

また、携帯機器30_1は、第２の家庭内ネットワークに属する対象機器10_3もアクセスの対象とすることができる。このとき、携帯機器30_1は、リソースとしての対象機器10_3に対してアクセスすることを認証するための属性証明書ACP_1'がホームゲートウェイ20_2によって発行され、ホームゲートウェイ20_1を介してこの属性証明書ACP_1'を受信すると、この属性証明書ACP_1'をＩＣカード等に格納すること等によって保持する。そして、携帯機器30_1は、対象機器10_3に対してアクセスしようと試みる際に、ＩＣカード等に格納された属性証明書ACP_1'を用いたログイン操作を行うことにより、この属性証明書ACP_1'をホームゲートウェイ20_1に対して送信して提示する。

【０１６９】

対象機器10_3は、第２の家庭内ネットワークを構成する機器であり、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書PKC_{T3}を保持し、この公開鍵証明書PKC_{T3}を用いてホームゲートウェイ20_2との間で相互認証を行う。また、対象機器10_3は、携帯機器30_2がアクセスする際に送信した属性証明書ACP_2をホームゲートウェイ20_2を介して受信し、この属性証明書ACP_2の検証を行う。さらに、対象機器10_3は、携帯機器30_1のアクセス対象とされた場合には、当該携帯機器30_1がアクセスする際に送信した属性証明書ACP_1'と、ホームゲートウェイ20_1が送信した属性証明書AC_Hとを、ホームゲートウェイ20_2を介して受信し、これらの属性証明書ACP_1'，AC_Hの検証を行う。

【０１７０】

ホームゲートウェイ20_2は、対象機器10_3が属する第２の家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能

する。ホームゲートウェイ２０$_2$は、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書ＰＫＣ$_{G2}$を保持し、この公開鍵証明書ＰＫＣ$_{G2}$を用いて対象機器１０$_3$、携帯機器３０$_2$、及び図示しない属性認証局ＡＡとの間で相互認証を行う。また、ホームゲートウェイ２０$_2$は、携帯機器３０$_2$に対して属性証明書ＡＣ$_{P2}$を発行する許可を与えるための属性証明書ＡＣ$_{L2}$が図示しない属性認証局ＡＡによって発行されると、この属性証明書ＡＣ$_{L2}$を保持し、この属性証明書ＡＣ$_{L2}$に基づいて、携帯機器３０$_2$に対して属性証明書ＡＣ$_{P2}$を発行する。さらに、ホームゲートウェイ２０$_2$は、携帯機器３０$_2$から送信された属性証明書ＡＣ$_{P2}$を受信すると、この属性証明書ＡＣ$_{P2}$を対象機器１０$_3$に対して送信して提示する。

【０１７１】

さらにまた、ホームゲートウェイ２０$_2$は、ホームゲートウェイ２０$_1$から属性証明書ＡＣ$_H$を受信すると、この属性証明書ＡＣ$_H$に基づいて、属性証明書ＡＣ$_{P1}$'をホームゲートウェイ２０$_1$に対して発行する。そして、ホームゲートウェイ２０$_2$は、ホームゲートウェイ２０$_1$を介して携帯機器３０$_1$から送信された属性証明書ＡＣ$_{P1}$'と、ホームゲートウェイ２０$_1$から送信された属性証明書ＡＣ$_H$とを受信すると、これらの属性証明書ＡＣ$_{P1}$', ＡＣ$_H$対象機器１０$_3$に対して送信して提示する。

【０１７２】

携帯機器３０$_2$は、第２の家庭内ネットワークに属する対象機器１０$_3$に対してアクセスするための機器であり、インターネット等のセキュアでないネットワークＮＴを介してホームゲートウェイ２０$_2$に対して接続可能とされる。携帯機器３０$_2$は、図示しない証明書発行認証局ＣＡによって発行された公開鍵証明書ＰＫＣ$_{M2}$を保持し、この公開鍵証明書ＰＫＣ$_{M2}$を用いてホームゲートウェイ２０$_2$との間で相互認証を行う。また、携帯機器３０$_2$は、リソースとしての対象機器１０$_3$に対してアクセスすることを認証するための属性証明書ＡＣ$_{P2}$がホームゲートウェイ２０$_2$によって発行されると、この属性証明書ＡＣ$_{P2}$をＩＣカード等に格納すること等によって保持する。そして、携帯機器３０$_2$は、対象機器１０$_3$に対してアクセスしようと試みる際に、ＩＣカード等に格納された

属性証明書$ＡＣ_{Ｐ２}$を用いたログイン操作を行うことにより、この属性証明書$ＡＣ_{Ｐ２}$をホームゲートウェイ２０_{2}に対して送信して提示する。

【０１７３】

このようなリモートアクセスシステムにおいては、上述した２つの属性証明書$ＡＣ_{Ｌ}$，$ＡＣ_{Ｐ}$の他、２つの属性証明書$ＡＣ_{Ｈ}$，$ＡＣ_{Ｐ１}$'が使用される。

【０１７４】

まず、属性証明書$ＡＣ_{Ｈ}$について説明する。

【０１７５】

属性証明書$ＡＣ_{Ｈ}$は、上述したように、アクセスすることができる他のネットワークにおけるエンティティ、具体的にはホームゲートウェイ２０_{2}を示す情報が記述されたものであり、図示しない属性認証局ＡＡによって署名されてホームゲートウェイ２０_{1}に対して発行されるものである。例えば、この属性証明書$ＡＣ_{Ｈ}$には、上述した属性（attributes）における各フィールドのうち、アクセス許可情報（Access Identity）等を用いて、アクセスすることができる他のネットワークにおけるエンティティとしてのホームゲートウェイ２０_{2}を示す情報を記述することができる。

【０１７６】

リモートアクセスシステムにおいては、アクセスすることができる他のネットワークにおけるエンティティとしてのホームゲートウェイ２０_{2}を示す情報を記述した属性証明書$ＡＣ_{Ｈ}$を、ホームゲートウェイ２０_{1}からの要求に応じて、ホームゲートウェイ２０_{2}によって発行することができる。これにより、リモートアクセスシステムにおいては、この属性証明書$ＡＣ_{Ｈ}$を保持したホームゲートウェイ２０_{1}を介して携帯機器３０_{1}が対象機器１０_{3}に対してアクセスすることが可能となる。

【０１７７】

つぎに、属性証明書$ＡＣ_{Ｐ１}$'について説明する。

【０１７８】

属性証明書$ＡＣ_{Ｐ１}$'は、上述した属性証明書$ＡＣ_{Ｐ}$と同様に、ある公開鍵証明書を保持している機器又はユーザに対する権限が記述されたものであり、ここ

では、公開鍵証明書PKC_{M1}を保持している携帯機器30_1に対する権限として、第２の家庭内ネットワークに属するリソースとしての対象機器10_3に対してアクセスすることを許可する旨の情報が記述されたものである。例えば、この属性証明書AC_{P1}'は、属性（attributes）については上述した属性証明書AC_Pと同様に、認証情報（Service Authentication Information）やアクセス許可情報（Access Identity）等を用いて、アクセスする対象、アクセスできる操作（権限）、及びアクセスするための認証情報がある場合には当該認証情報が記述される一方で、プロシキ情報（Proxy Info）としては、当該属性証明書AC_{P1}'を経由させる２つのホームゲートウェイ20_1，20_2を識別するためのアドレスや識別子等の情報が記述されたものとなる。

【０１７９】

このように、リモートアクセスシステムにおいては、携帯機器30_1に対する権限として、第２の家庭内ネットワークに属するリソースとしての対象機器10_3に対してアクセスすることを許可する旨の情報が記述されるとともに、プロシキ情報として、２つのホームゲートウェイ20_1，20_2の情報が記述された属性証明書AC_{P1}'を、ホームゲートウェイ20_2からホームゲートウェイ20_1を介して携帯機器30_1に対して発行することができる。これにより、リモートアクセスシステムにおいては、対象機器10_3が、この属性証明書AC_{P1}'をホームゲートウェイ20_2を介して受信した場合には、プロシキ情報におけるターゲットを検証し、且つ、２つのホームゲートウェイ20_1，20_2を介して受信した属性証明書であることを検証することになる。

【０１８０】

さて、このようなリモートアクセスシステムにおいては、具体的には、先に図１１に示したように、準備フェーズＰ１、登録フェーズＰ２、アクセスフェーズＰ３、アクセス削除フェーズＰ４、及びアクセス変更フェーズＰ５が行われる。なお、以下では、携帯機器30_1によって第２の家庭内ネットワークに属する対象機器10_3に対してアクセスするものとして説明する。

【０１８１】

まず、準備フェーズＰ１について説明する。

【０１８２】

リモートアクセスシステムにおいては、当該リモートアクセスシステムを構築するための準備フェーズＰ１として、各エンティティが相互認証可能となるように、証明書発行認証局ＣＡにより、各エンティティに対して認証のための公開鍵証明書を発行する。すなわち、リモートアクセスシステムにおいては、上述したように、各エンティティの製造時等に、証明書発行認証局ＣＡにより、公開鍵証明書PKC_{T1}，PKC_{T2}，PKC_{T3}を、それぞれ、対象機器10_1，10_2，10_3に対して発行するとともに、公開鍵証明書PKC_{G1}，PKC_{G2}を、それぞれ、ホームゲートウェイ20_1，20_2に対して発行するとともに、公開鍵証明書PKC_{M1}，PKC_{M2}を、それぞれ、携帯機器30_1，30_2に対して発行する。

【０１８３】

リモートアクセスシステムは、このような準備フェーズＰ１を経ることにより、各エンティティが相互認証可能な状態に構築される。

【０１８４】

つぎに、登録フェーズＰ２について説明する。

【０１８５】

リモートアクセスシステムにおいては、任意の携帯機器としての携帯機器３０をリソースに対してアクセスする機器として登録するための登録フェーズＰ２として、図１７に示す工程が行われる。

【０１８６】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ４１において、属性認証局ＡＡにより、上述した準備フェーズＰ１にて証明書発行認証局ＣＡによって発行されてホームゲートウェイ20_1に保持されている公開鍵証明書PKC_{G1}を用いて、ホームゲートウェイ20_1との間で相互認証を行う。この相互認証は、ホームゲートウェイ20_1自体に対する認証であり、ホームゲートウェイ20_1が正当なものであるか否かを認証するためのものである。

【０１８７】

続いて、リモートアクセスシステムにおいては、ステップＳ４２において、属性認証局ＡＡにより、ホームゲートウェイ２０_{1}がユーザサイドに渡ってから初回接続時等に、携帯機器３０_{1}に対して属性証明書$ＡＣ_{Ｐ１}$を発行する許可を与えるための属性証明書$ＡＣ_{Ｌ１}$を、ホームゲートウェイ２０_{1}に対して発行する。この際、リモートアクセスシステムにおいては、ホームゲートウェイ２０_{1}が他のホームゲートウェイ２０_{2}に対してアクセスする場合には、属性認証局ＡＡにより、ホームゲートウェイ２０_{2}に対してアクセスできる旨の情報が記述された属性証明書$ＡＣ_{Ｈ}$を、ホームゲートウェイ２０_{1}に対して発行する。これにともない、ホームゲートウェイ２０_{1}は、属性認証局ＡＡから送信された２つの属性証明書$ＡＣ_{Ｌ１}$，$ＡＣ_{Ｈ}$を保持する。

【０１８８】

続いて、リモートアクセスシステムにおいては、ステップＳ４３において、ホームゲートウェイ２０_{1}により、ユーザからの指示にしたがい、接続する機器、すなわち、対象機器１０_{1}，１０_{2}のそれぞれの情報を登録するとともに、その対象機器１０_{1}，１０_{2}のそれぞれに対してリモートからアクセスしてもよい携帯機器３０_{1}に対して上述したプロシキ情報を記述した属性証明書$ＡＣ_{Ｐ１}$を発行する。

【０１８９】

続いて、リモートアクセスシステムにおいては、携帯機器３０_{1}から他のホームゲートウェイ２０_{2}を介して対象機器１０_{3}に対してアクセスしたい場合には、ステップＳ４４において、ホームゲートウェイ２０_{1}により、保持している属性証明書$ＡＣ_{Ｈ}$を他のホームゲートウェイ２０_{2}に対して送信して提示し、上述したプロシキ情報を記述した属性証明書$ＡＣ_{Ｐ１}'$を発行してもらう。これにともない、ホームゲートウェイ２０_{2}は、属性証明書$ＡＣ_{Ｐ１}'$を発行し、この属性証明書$ＡＣ_{Ｐ１}'$をホームゲートウェイ２０_{1}に対して送信する。

【０１９０】

続いて、リモートアクセスシステムにおいては、ステップＳ４５において、携帯機器３０_{1}により、上述した準備フェーズＰ１にて証明書発行認証局ＣＡによって発行されて保持している公開鍵証明書$ＰＫＣ_{Ｍ１}$を用いて、ホームゲートウ

エイ２０$_1$との間で相互認証を行う。

【０１９１】

そして、リモートアクセスシステムにおいては、ステップＳ４６において、携帯機器３０$_1$により、ホームゲートウェイ２０$_1$から送信された属性証明書ＡＣ$_{P1}$，ＡＣ$_{P1}$'をＩＣカード等に格納して保持し、一連の登録フェーズＰ２を終了する。

【０１９２】

リモートアクセスシステムにおいては、このような一連の工程からなる登録フェーズＰ２を経ることにより、リソースに対してアクセスする機器として、携帯機器３０$_1$を登録することができる。このようにしてリソースに対してアクセスする携帯機器３０$_1$の登録がされたリモートアクセスシステムにおいては、登録された携帯機器３０$_1$が任意の操作を行うことが可能となる。

【０１９３】

つぎに、アクセスフェーズＰ３について説明する。

【０１９４】

リモートアクセスシステムにおいては、登録された携帯機器３０$_1$がリソースに対してアクセスする際には、アクセスフェーズＰ３として、図１８に示す工程が行われる。

【０１９５】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップＳ５１において、携帯機器３０$_1$により、保持している公開鍵証明書ＰＫＣ$_{M1}$を用いて、ホームゲートウェイ２０$_1$との間で相互認証を行う。

【０１９６】

続いて、リモートアクセスシステムにおいては、ステップＳ５２において、携帯機器３０$_1$により、保持している属性証明書ＡＣ$_{P1}$，ＡＣ$_{P1}$'のいずれかをホームゲートウェイ２０$_1$に対して送信して提示する。具体的には、リモートアクセスシステムにおいては、対象機器１０$_1$，１０$_2$のいずれか又は双方に対してアクセスする場合には、携帯機器３０$_1$により、保持している属性証明書ＡＣ$_{P1}$をホームゲートウェイ２０$_1$に対して送信して提示する一方で、対象機器

１０$_3$に対してアクセスする場合には、携帯機器３０$_1$により、保持している属性証明書ＡＣ$_{P1}$'をホームゲートウェイ２０$_1$に対して送信して提示する。

【０１９７】

ここで、リモートアクセスシステムにおいては、携帯機器３０$_1$により、保持している属性証明書ＡＣ$_{P1}$をホームゲートウェイ２０$_1$に対して送信して提示した場合には、先に図１３中ステップＳ１３乃至ステップＳ１７に示した処理と同様の処理を行うが、ここでは、携帯機器３０$_1$は、保持している属性証明書ＡＣ$_{P1}$'をホームゲートウェイ２０$_1$に対して送信して提示するものとして説明する。

【０１９８】

リモートアクセスシステムにおいては、ステップＳ５３において、ホームゲートウェイ２０$_1$により、携帯機器３０$_1$から提示された属性証明書ＡＣ$_{P1}$'におけるプロシキ情報を検証し、アクセス対象の機器が自己の配下にある第１の家庭内ネットワークとは異なる第２の家庭内ネットワークに属する対象機器１０$_3$である旨を把握すると、２つの属性証明書ＡＣ$_{P1}$'，ＡＣ$_H$を、第２の家庭内ネットワークを司るホームゲートウェイ２０$_2$に対して送信して提示する。

【０１９９】

続いて、リモートアクセスシステムにおいては、ステップＳ５４において、ホームゲートウェイ２０$_2$により、ホームゲートウェイ２０$_1$から提示された２つの属性証明書ＡＣ$_{P1}$'，ＡＣ$_H$の内容に基づいて、当該属性証明書ＡＣ$_{P1}$'，ＡＣ$_H$を、アクセスする対象として指定された機器、すなわち、対象機器１０$_3$に対して送信して提示する。

【０２００】

続いて、リモートアクセスシステムにおいては、ステップＳ５５において、対象機器１０$_3$により、ホームゲートウェイ２０$_2$から送信された２つの属性証明書ＡＣ$_{P1}$'，ＡＣ$_H$を受信し、上述したプロシキ情報や属性といった当該属性証明書ＡＣ$_{P1}$'，ＡＣ$_H$の内容を検証する。

【０２０１】

リモートアクセスシステムにおいては、ステップＳ５６において、属性証明書

AC_{P1}'，AC_Hの検証結果が正当なものであった場合には、ステップＳ５７において、対象機器10_3によって携帯機器30_1のアクセスを許可し、一連のアクセスフェーズＰ３を終了する。一方、リモートアクセスシステムにおいては、ステップＳ５６において、属性証明書AC_{P1}'，AC_Hの検証結果が不当なものであった場合には、ステップＳ５８において、対象機器10_3によって携帯機器30_1のアクセスを拒否し、一連のアクセスフェーズＰ３を終了する。

【０２０２】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセスフェーズＰ３を経ることにより、対象機器10_3によって携帯機器30_1の権限を判別することができ、アクセスが許可された携帯機器30_1は、任意の操作を行うことが可能となる。

【０２０３】

つぎに、アクセス削除フェーズＰ４について説明する。

【０２０４】

リモートアクセスシステムにおいては、任意の携帯機器をリソースに対してアクセスする機器から除外したい場合には、アクセス削除フェーズＰ４として、図１９に示す工程が行われる。なお、リモートアクセスシステムにおいては、携帯機器30_1が対象機器10_1，10_2をアクセス対象としている場合には、先に図１４に示した処理と同様の処理を行えばよく、ここでは、携帯機器30_1が対象機器10_3をアクセス対象としており、携帯機器30_1を対象機器10_3に対してアクセスする機器から除外したい場合について説明する。

【０２０５】

まず、リモートアクセスシステムにおいては、図１９に示すように、ステップＳ６１において、ホームゲートウェイ20_1により、ユーザからの指示にしたがい、対象機器10_3に対してリモートからアクセスしてもよい携帯機器30_1に対して発行した属性証明書AC_{P1}'に対するＣＲＬ（ＡＣＲＬ）の作成をホームゲートウェイ20_2に対して要求する。

【０２０６】

続いて、リモートアクセスシステムにおいては、ステップＳ６２において、ホ

ームゲートウェイ２０$_2$により、ホームゲートウェイ２０$_1$からの要求にしたがい、属性証明書ＡＣ$_{P1}$'に対するＣＲＬ（ＡＣＲＬ）を作成する。

【０２０７】

そして、リモートアクセスシステムにおいては、ステップＳ６３において、ホームゲートウェイ２０$_2$により、作成した属性証明書ＡＣ$_{P1}$'に対するＣＲＬ（ＡＣＲＬ）をホームゲートウェイ２０$_1$に対して送信して配布する。これにともない、ホームゲートウェイ２０$_1$は、ホームゲートウェイ２０$_2$から送信された属性証明書ＡＣ$_{P1}$'に対するＣＲＬ（ＡＣＲＬ）を保持する。

【０２０８】

このように、リモートアクセスシステムにおいては、属性証明書ＡＣ$_{P1}$'に対するＣＲＬ（ＡＣＲＬ）をホームゲートウェイ２０$_2$によって作成することにより、携帯機器３０$_1$からホームゲートウェイ２０$_1$を介して対象機器１０$_3$に対してアクセスがあった場合には、ホームゲートウェイ２０$_1$によってアクセスを拒否することができ、携帯機器３０$_1$をリソースに対してアクセスする機器から除外することができる。

【０２０９】

また、リモートアクセスシステムにおいては、上述したように、正当なユーザが自らの意思で携帯機器３０をリソースに対してアクセスする機器から除外したい場合等には、ステップＳ６３の処理に続いて、先に図１４中ステップＳ２２乃至ステップＳ２４に示した処理と同様の処理を行うようにしてもよい。

【０２１０】

すなわち、リモートアクセスシステムにおいては、ステップＳ６４において、携帯機器３０$_1$により、保持している公開鍵証明書ＰＫＣ$_{M1}$を用いて、ホームゲートウェイ２０$_1$との間で相互認証を行う。

【０２１１】

続いて、リモートアクセスシステムにおいては、ステップＳ６５において、ホームゲートウェイ２０$_1$からの指示にしたがい、携帯機器３０$_1$により、保持している属性証明書ＡＣ$_{P1}$'を削除する。

【０２１２】

そして、リモートアクセスシステムにおいては、ステップＳ６６において、ホームゲートウェイ２０$_1$により、ステップＳ６３にて保持したＣＲＬ（ＡＣＲＬ）を削除し、一連のアクセス削除フェーズＰ４を終了する。

【０２１３】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス削除フェーズＰ４を経ることにより、携帯機器３０$_1$をリソースとしての対象機器１０$_3$に対してアクセスする機器から除外することができる。

【０２１４】

なお、リモートアクセスシステムにおいては、対象機器１０$_3$の側の都合により、携帯機器３０$_1$を当該対象機器１０$_3$に対してアクセスする機器から除外したい場合には、ステップＳ６１の処理をスキップし、ユーザからの指示にしたがい、ステップＳ６２からの処理を行えばよいことになる。

【０２１５】

最後に、アクセス変更フェーズＰ５について説明する。

【０２１６】

リモートアクセスシステムにおいては、任意の携帯機器の権限を変更したい場合には、アクセス変更フェーズＰ５として、図２０に示す工程が行われる。なお、リモートアクセスシステムにおいては、第１の家庭内ネットワークにおけるリソースに対する携帯機器３０$_1$の権限を変更したい場合には、先に図１５に示した処理と同様の処理を行えばよく、ここでは、第２の家庭内ネットワークにおけるリソースに対する携帯機器３０$_1$の権限を変更したい場合について説明する。

【０２１７】

まず、リモートアクセスシステムにおいては、図２０に示すように、ステップＳ７１において、ホームゲートウェイ２０$_1$により、ユーザからの指示にしたがい、保持している属性証明書ＡＣ$_H$を他のホームゲートウェイ２０$_2$に対して送信して提示し、プロシキ情報を記述した新たな属性証明書ＡＣ$_{P1}$'を発行してもらう。これにともない、ホームゲートウェイ２０$_2$は、新たな属性証明書ＡＣ$_{P1}$'を発行し、この属性証明書ＡＣ$_{P1}$'をホームゲートウェイ２０$_1$に対して送信する。

【０２１８】

続いて、リモートアクセスシステムにおいては、ステップＳ７２において、携帯機器３０$_1$により、保持している公開鍵証明書ＰＫＣ$_{M1}$を用いて、ホームゲートウェイ２０$_1$との間で相互認証を行う。

【０２１９】

そして、リモートアクセスシステムにおいては、ステップＳ７３において、携帯機器３０$_1$により、ホームゲートウェイ２０$_1$から送信された新たな属性証明書ＡＣ$_{P1}$'を、元の属性証明書ＡＣ$_{P1}$'と置換してＩＣカード等に格納して保持し、一連のアクセス変更フェーズＰ５を終了する。

【０２２０】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス変更フェーズＰ５を経ることにより、携帯機器３０$_1$の権限を変更することができる。これにより、リモートアクセスシステムにおいては、携帯機器３０$_1$が新たな任意の操作を行うことが可能となる。

【０２２１】

以上のように、リモートアクセスシステムは、プロシキ情報が記述された属性証明書ＡＣ$_{P1}$'を用いて、通常では携帯機器３０$_1$からはアクセスすることができない第２の家庭内ネットワークにおけるリソースに対する権限管理を行うことができる。

【０２２２】

このように、本発明は、携帯機器が通常アクセスできるネットワークの入り口としてのホームゲートウェイが当該携帯機器に対して属性証明書ＡＣ$_P$を発行するのではなく、他のネットワークの入り口としてのホームゲートウェイといった任意のエンティティが属性証明書ＡＣ$_P$を発行するものであってもよく、ホームゲートウェイは、属性証明書ＡＣ$_P$の内容を検証できるものであればよい。

【０２２３】

また、上述した実施の形態では、家庭内ネットワークにおけるリソースに対してアクセスするものとして説明したが、本発明は、任意のネットワークに対して適用することができる。

【０２２４】

さらに、上述した実施の形態では、リソースに対してアクセス機器として携帯機器を用いて説明したが、本発明は、このような機器としては、携帯型の機器に限らずいかなる機器をも適用することができる。

【０２２５】

さらにまた、本発明は、各エンティティの動作をハードウェアで実現するのみならず、ソフトウェアで実現することもできる。本発明は、ソフトウェアで実現する場合には、例えば各エンティティが備えるＣＰＵ（Central Processing Unit）によって上述したリモートアクセスを行うためのリモートアクセスプログラムを実行することにより、各機能を実現することができる。このリモートアクセスプログラムは、例えばいわゆるコンパクトディスク（Compact Disc）等の所定の記録媒体やインターネット等の伝送媒体によって提供することができる。

【０２２６】

このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【０２２７】

【発明の効果】

以上詳細に説明したように、本発明にかかるリモートアクセスシステムは、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器と、このアクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当する機器であるゲートウェイ機器と、少なくともリソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持し、アクセス対象機器に対してアクセスするアクセス機器とを備え、アクセス機器は、権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器は、アクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対

象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器は、ゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【０２２８】

したがって、本発明にかかるリモートアクセスシステムは、少なくともリソースに対する権限とゲートウェイ機器の情報とを、権限及び経由情報記述属性証明書に記述し、この権限及び経由情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証することにより、リソース毎に、権限単位での制御を容易に行うことができ、また、権限及び経由情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることができる。

【０２２９】

また、本発明にかかるリモートアクセス方法は、所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持させ、アクセス機器によって権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器によってアクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器によってゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【０２３０】

したがって、本発明にかかるリモートアクセス方法は、少なくともリソースに

対する権限とゲートウェイ機器の情報とを、権限及び経由情報記述属性証明書に記述し、この権限及び経由情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証することにより、リソース毎に、権限単位での制御を容易に行うことが可能となり、また、権限及び経由情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることが可能となる。

【０２３１】

さらに、本発明にかかるリモートアクセスプログラムは、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【０２３２】

したがって、本発明にかかるリモートアクセスプログラムは、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経由情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経由情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証することにより、このリモートアクセスプログラムが実装された機器が、リソース毎に、権限単位での制御を容易に行うことを可能とし、また、権限及び経由情報記述属性証明書の送付ルートを確認することを可能とし、セキュリティを向上させることを可能とする。

【０２３３】

さらにまた、本発明にかかるリモートアクセスプログラムが記録された記録媒

体は、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムが記録された記録媒体であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書が保持されており、リモートアクセスプログラムは、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【０２３４】

したがって、本発明にかかるリモートアクセスプログラムが記録された記録媒体は、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経由情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経由情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証するリモートアクセスプログラムを提供することができる。そのため、このリモートアクセスプログラムが実装された機器は、リソース毎に、権限単位での制御を容易に行うことができ、また、権限及び経由情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることができる。

【図面の簡単な説明】

【図１】

公開鍵証明書のフォーマットを説明する図である。

【図２】

公開鍵証明書のフォーマットを説明する図であって、図１に示す項目に続く残りの項目を説明する図である。

【図３】

属性証明書のフォーマットを説明する図である。

【図４】

属性証明書のフォーマットを説明する図であって、図３に示す項目に続く残りの項目を説明する図である。

【図５】

権限プロキシ機能を説明するための図である。

【図６】

本発明の実施の形態として示すリモートアクセスシステムの概念図である。

【図７】

図４に示す属性証明書の項目のうち、属性における各フィールドの抜粋を示す図である。

【図８】

ロールの概念を用いた権限管理の手法について説明する図である。

【図９】

図４に示す属性証明書の項目のうち、拡張情報における各フィールドの抜粋を示す図である。

【図１０】

図４に示す属性証明書の項目のうち、拡張情報におけるプロシキ情報の具体的な記述内容を説明する図である。

【図１１】

同リモートアクセスシステムにて行われる各フェーズを説明するためのフローチャートである。

【図１２】

同リモートアクセスシステムにおける登録フェーズとしての一連の工程を説明するためのフローチャートである。

【図１３】

同リモートアクセスシステムにおけるアクセスフェーズとしての一連の工程を説明するためのフローチャートである。

【図１４】

同リモートアクセスシステムにおけるアクセス削除フェーズとしての一連の工

程を説明するためのフローチャートである。

【図１５】

同リモートアクセスシステムにおけるアクセス変更フェーズとしての一連の工程を説明するためのフローチャートである。

【図１６】

本発明の他の実施の形態として示すリモートアクセスシステムの概念図である。

【図１７】

同リモートアクセスシステムにおける登録フェーズとしての一連の工程を説明するためのフローチャートである。

【図１８】

同リモートアクセスシステムにおけるアクセスフェーズとしての一連の工程を説明するためのフローチャートである。

【図１９】

同リモートアクセスシステムにおけるアクセス削除フェーズとしての一連の工程を説明するためのフローチャートであって、携帯機器を他のネットワークに属する対象機器に対してアクセスする機器から除外する場合における一連の工程を説明するためのフローチャートである。

【図２０】

同リモートアクセスシステムにおけるアクセス変更フェーズとしての一連の工程を説明するためのフローチャートであって、他のネットワークにおけるリソースに対する携帯機器の権限を変更する場合における一連の工程を説明するためのフローチャートである。

【符号の説明】

10_1，10_2，10_3 対象機器、 20，20_1，20_2 ホームゲートウェイ、 30，30_1，30_2 携帯機器、 AA 属性認証局、 AC，AC_H，AC_L，AC_{L1}，AC_{L2}，AC_P，AC_{P1}，AC_{P2}，AC_{P1}' 属性証明書、 AS 権限主張側サーバ、 AU_{11}，AU_{12}，・・・，AU_{21}，AU_{22}，・・・ 権限、 CA 証明書発行認証局、 CL クライ

アント、 M_1，M_2，M_3 個人、 ＮＴ ネットワーク、 PKC_G，PKC_{G1}，PKC_{G2}，PKC_M，PKC_{M1}，PKC_{M2}，PKC_{T1}，PKC_{T2}，PKC_{T3} 公開鍵証明書、 R_1，R_2 ロール、 ＲＡ 役割認証局、 ＲＡＡＣ 役割割当証明書、 ＲＳＡＣ 役割定義証明書、 ＶＲ 権限検証側サーバ

【書類名】　図面

【図１】

項目	説明
Version 1	
version	証明書のフォーマットのバージョン
serial Number	証明書発行認証局によって設定される証明書のシリアルナンバ
signature algorithm Identifier algorithm parameters	証明書の署名アルゴリズム、及びそのパラメータ
issuer	証明書発行認証局の名称 (Distinguished Name形式)
validity not Before not After	証明書の有効期限 開始日時 終了日時
subject	ユーザを識別する名前
subject Public Key Info algorithm subject Public key	ユーザの公開鍵情報 鍵アルゴリズム 鍵情報
Version 3	
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	証明書発行認証局の署名確認用の鍵識別 鍵識別番号（8進数） 証明書発行認証局の名称 (General Name形式) 認証番号
subject key Identifier	複数の鍵の証明をする場合の各鍵の識別子
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key Cert Sign (6)CRL Sign (7)encipher Only (8)decipher Only	鍵の使用目的を指定 (0)ディジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配送用 (5)認証の署名確認用 (6)失効リストの署名確認用 (7)鍵交換時データの暗号化にのみ利用 (8)鍵交換時データの復号にのみ利用
private Key Usage Period not Before not After	ユーザに格納されている秘密鍵の有効期限

公開鍵証明書のフォーマットの説明図

【図２】

Certificate Policy policy Identifier policy Qualifiers	証明書発行認証局の 証明書発行ポリシー ポリシーID 認証基準
policy Mappings issuer Domain Policy subject Domain Policy	証明書発行認証局を認証する場合にのみ必要。証明書発行認証局のポリシーと被認証ポリシーとのマッピングを規定。
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ディレクトリ（X.500）のアトリビュートを定義。コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。
subject Alt Name	ユーザの別名（GN形式）
issuer Alt Name	証明書発行者の別名
subject Directory Attributes	ユーザの任意の属性
basic Constraints CA path Len Constraint	証明対象の公開鍵が証明書発行認証局の署名用か、ユーザのものかを区別
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	被認証者が証明書発行認証局である場合（CA認証）にのみ使用
policy Constraints require Explicit Policy inhibit Policy Mapping	認証パスの残りに対する明確な認証ポリシーID、禁止ポリシーマップを要求する制限を記述
CRL Distribution Points	ユーザが証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照ポイントを記述
署名	発行者の署名

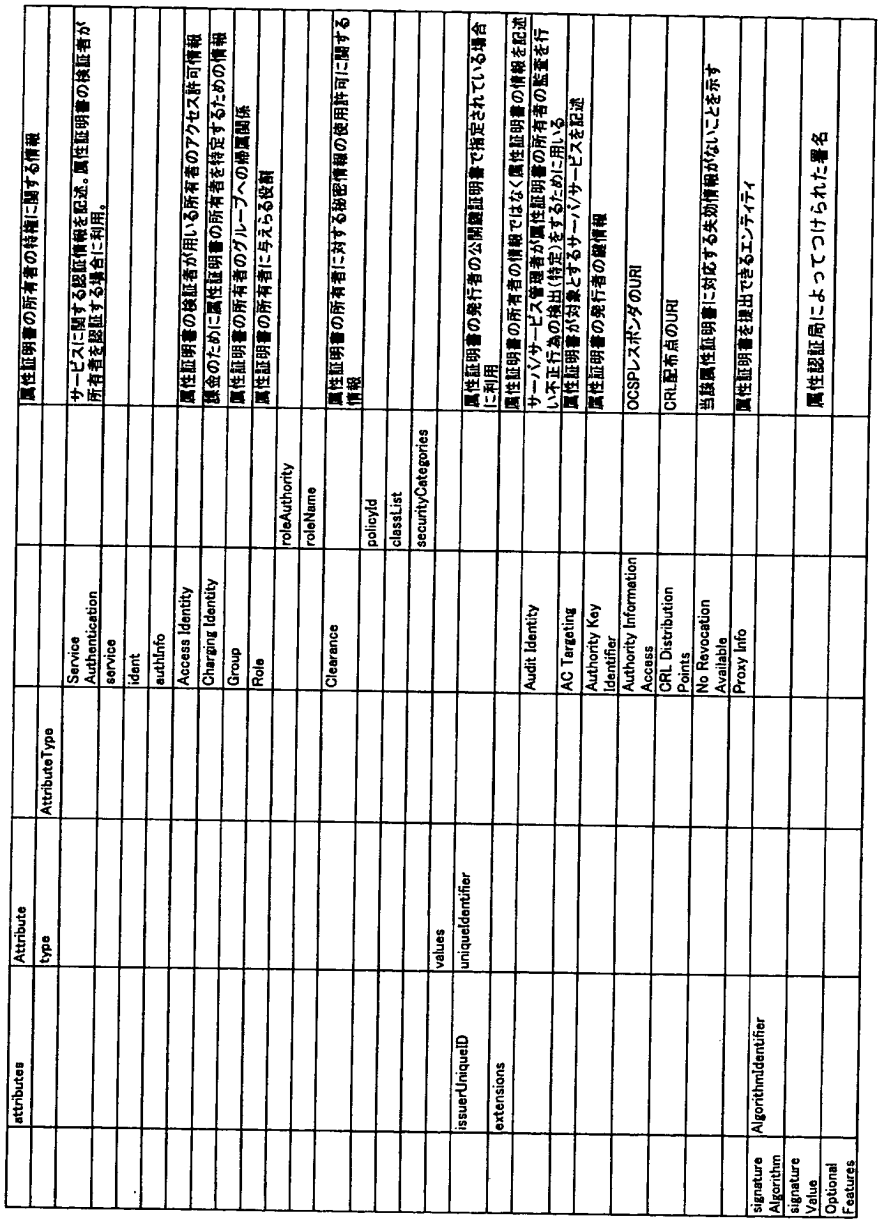
公開鍵証明書のフォーマットの説明図

【図３】

項目						説明
acinfo	AttributeCertificateInfo					
	version	AttCertVersion				属性証明書のフォーマットのバージョン
	holder	Holder				属性証明書が結び付けられた公開鍵証明書の所有者を特定
		baseCertificateID	issuerSerial			属性証明書の所有者の公開鍵証明書の発行者名
			issuer			属性証明書の所有者の公開鍵証明書のシリアル番号
			serial			属性証明書の所有者の公開鍵証明書の発行者固有識別子
			issuerUID			属性証明書の所有者の名称
		entityName				将来、属性証明書が識別情報や公開鍵証明書にリンクされていない場合を想定
		objectDigestInfo	objectDigestInfo			
			digestedObjectType			
			otherObjectTypeID			
			digestAlgorithm			
			objectDigest			
	issuer	AttCertIssuer				属性証明書に署名した発行者の名前を指定
		v2Form	V2Form			
			issuerName			属性証明書の発行者名
			baseCertificateID			
			objectDigestInfo			
	signature	Algorithmidentifier				属性証明書の署名を有効にするために使用するアルゴリズム識別子
	serialNumber	CertificateSerialNumber				属性認証局が各証明書に割り振るシリアルナンバ
	attrCertValidityPeriod	AttCertValidityPeriod				属性証明書の有効期限
		notBefore				開始日時
		notAfter				終了日時

属性証明書のフォーマットの説明図

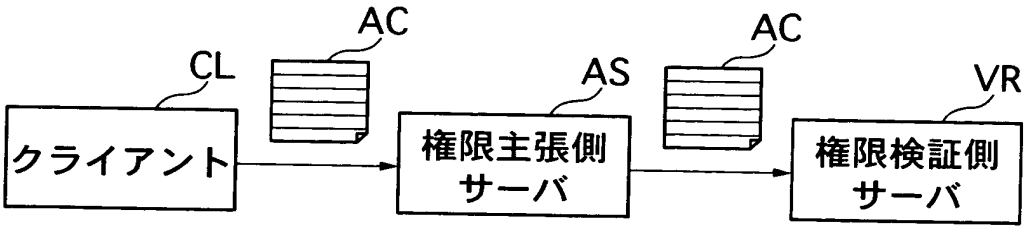
【図４】



attributes	Attribute				属性証明書の所有者の特権に関する情報
	type	AttributeType			
			Service Authentication		サービスに関する認証情報を記述。属性証明書の検証者が所有者を認証する場合に利用。
			service		
			ident		
			authInfo		
			Access Identity		属性証明書の検証者が用いる所有者のアクセス許可情報
			Charging Identity		課金のために属性証明書の所有者を特定するための情報
			Group		属性証明書の所有者のグループへの帰属関係
			Role		属性証明書の所有者に与えられる役割
				roleAuthority	
				roleName	
			Clearance		属性証明書の所有者に対する秘密情報の使用許可に関する情報
				policyId	
				classList	
				securityCategories	
	values				
	issuerUniqueID	uniqueIdentifier			属性証明書の発行者の公開鍵証明書で指定されている場合に利用
	extensions				属性証明書の所有者の情報ではなく属性証明書の情報を記述
			Audit Identity		サーバ/サービス管理者が属性証明書の所有者の監査を行い不正行為の検出(特定)をするために用いる
			AC Targeting		属性証明書が対象とするサーバ/サービスを記述
			Authority Key Identifier		属性証明書の発行者の鍵情報
			Authority Information Access		OCSPレスポンダのURI
			CRL Distribution Points		CRL配布点のURI
			No Revocation Available		当該属性証明書に対応する失効情報がないことを示す
			Proxy Info		属性証明書を提出できるエンティティ
Signature Algorithm	AlgorithmIdentifier				
signature Value					属性認証局によってつけられた署名
Optional Features					

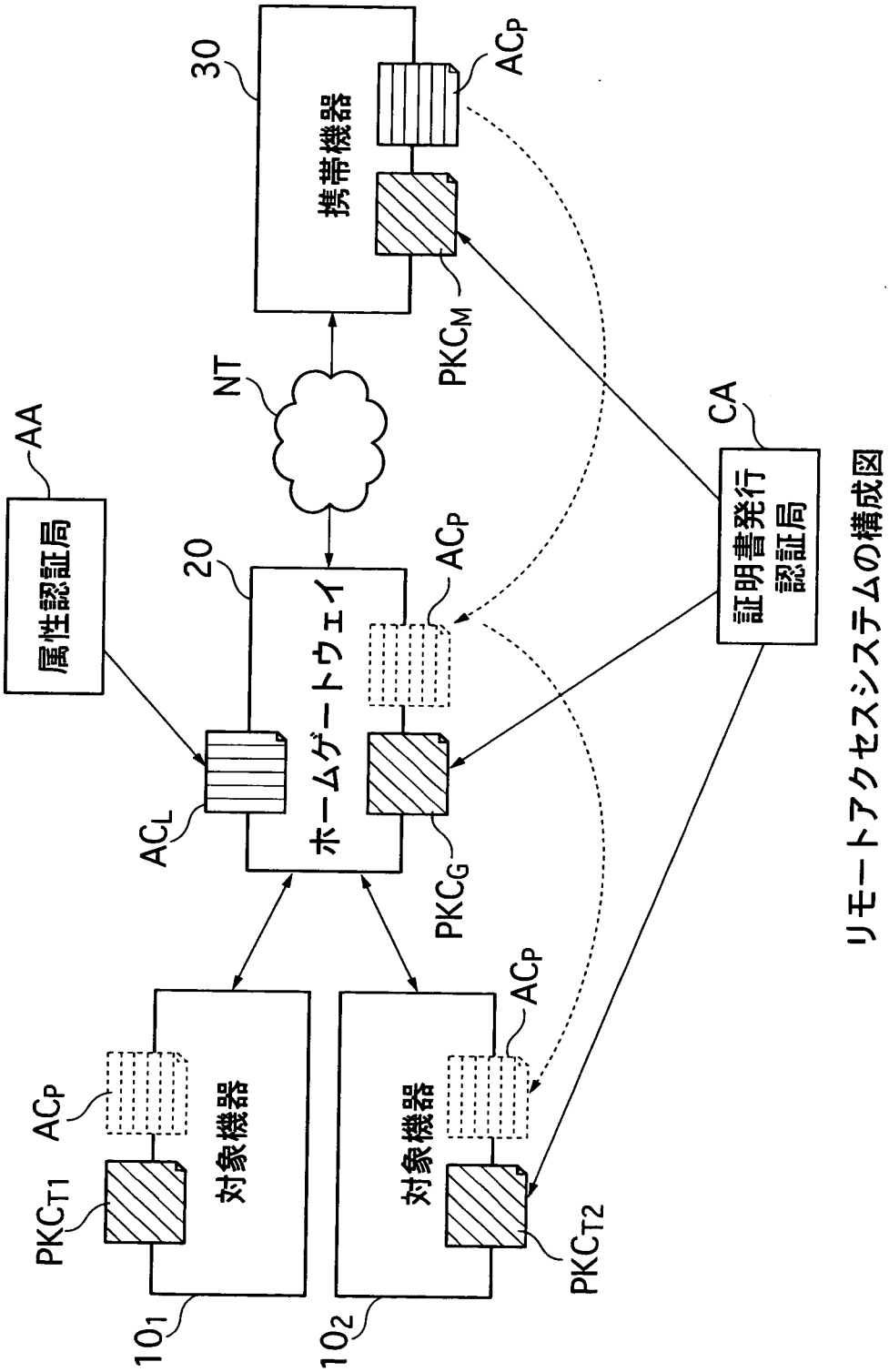
属性証明書のフォーマットの説明図

【図５】



権限プロキシ機能の説明図

【図６】



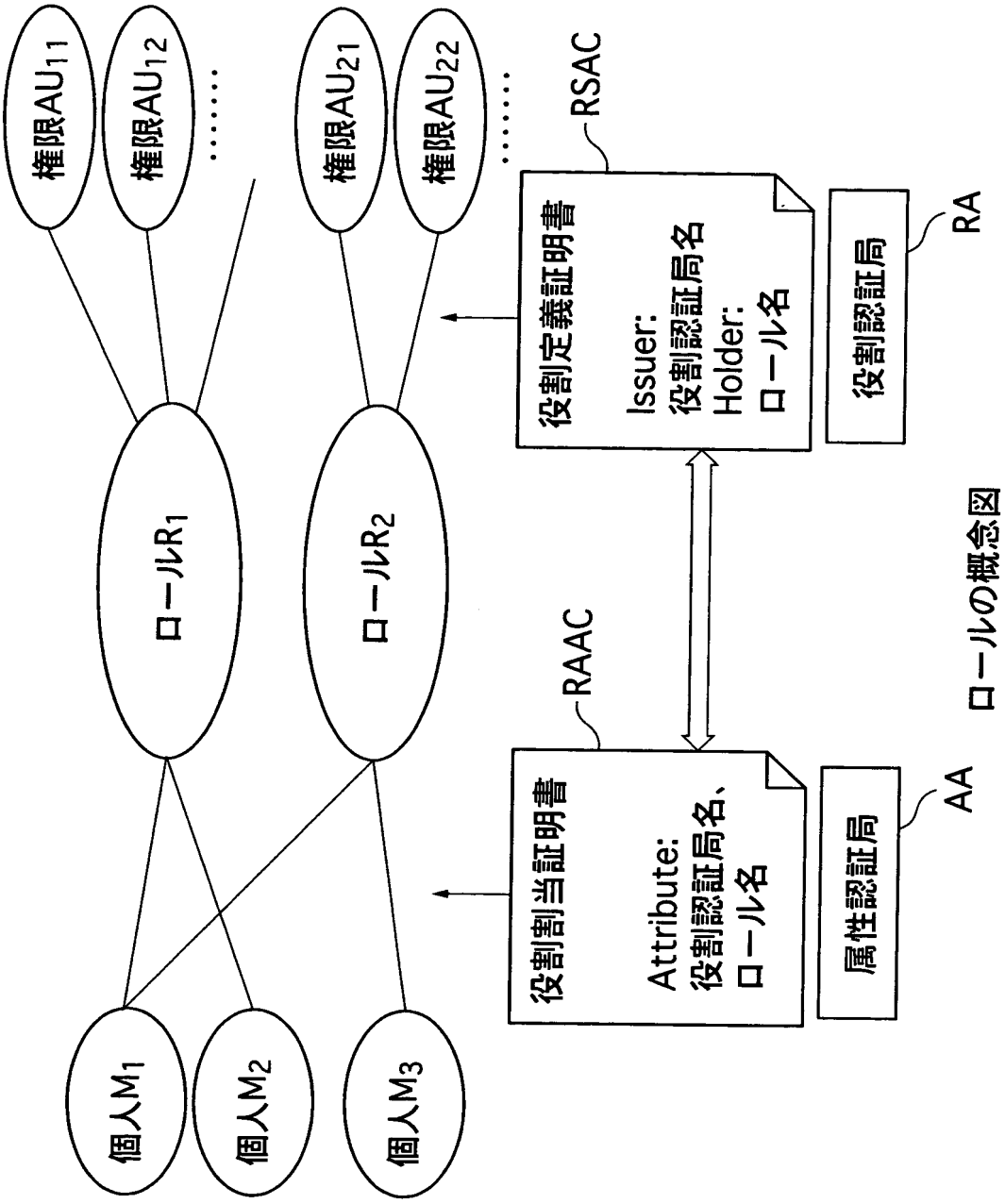
リモートアクセスシステムの構成図

【図７】

項目	OID	値
Service Authentication Information	id-aca 1	サービス又は認証時に必要とされる情報
Access Identity	id-aca 2	所有者の属性を検証する際に所有者を識別するもの
Charging Identity	id-aca 3	サービスの課金に利用するID
Group	id-aca 4	所有者が所属するグループ情報
Role	id-at 72	役割認証局名、ロール名

属性証明書のフォーマットの説明図

【図８】


権限AU11
権限AU12
権限AU21
権限AU22
ロールR1
ロールR2
個人M1
個人M2
個人M3
RSAC
役割定義証明書
Issuer:
役割認証局名
Holder:
ロール名
役割認証局
RA
RAAC
役割割当証明書
Attribute:
役割認証局名、
ロール名
属性認証局
AA

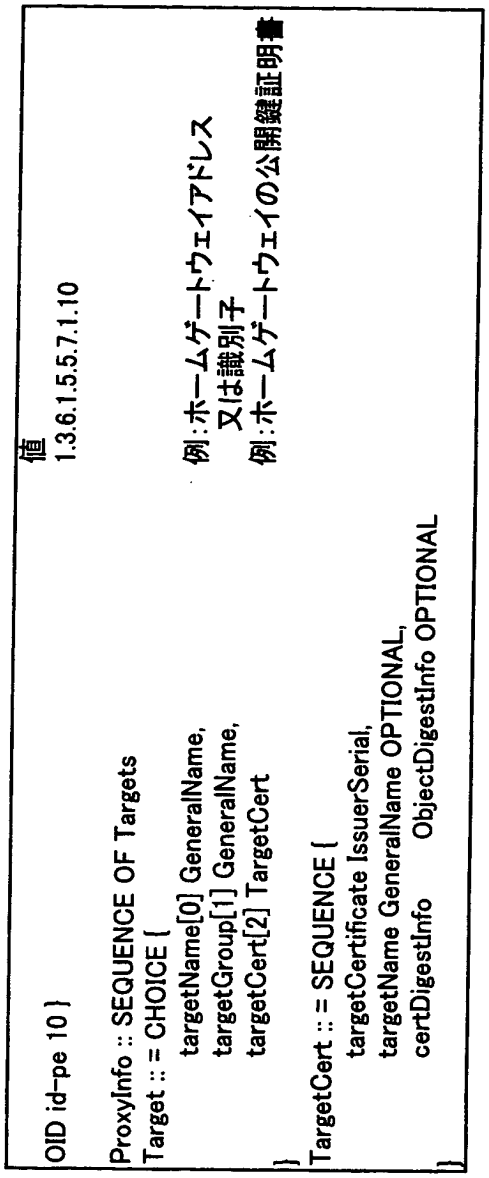
ロールの概念図

【図９】

項目	OID	値
Authority Information Access		属性証明書の発行者情報、OCSP情報
Authority Key Identifier		属性認証局の公開鍵情報
CRL Distribution Points		CRL配布点のURI
Audit Identity		監査用の属性証明書所有者ID(ログ追跡に用いる;匿名性があるが属性認証局にある情報を合わせれば本人の特定ができる)
Time Specification		権限が有効な時間帯
Targeting Information		属性証明書を受け取れるサーバ名
Proxy Info		可能なプロキシ
User Notice		権限所有者や権限検証者への伝達情報
権限ポリシー		policy authority名、文字列又はOIDの値
SOA (Source of Authority;検証者が信頼するエンティティ、PKIでのルートCA,Trust anchorに相当するDelegation(属性認証局のChain)でのトップ(通常、属性認証局は1つなので、属性認証局=SOA))		SOAになれる権限 SOAの証明書である旨の記述
権限委譲		権限を他のエンティティに委譲する際の委譲条件等の記述
属性の廃棄		CRL配布点のURI
		失効をサポートしていない旨の記述
Role		役割定義証明書を示す(Role authority名、ロール名を文字列で)

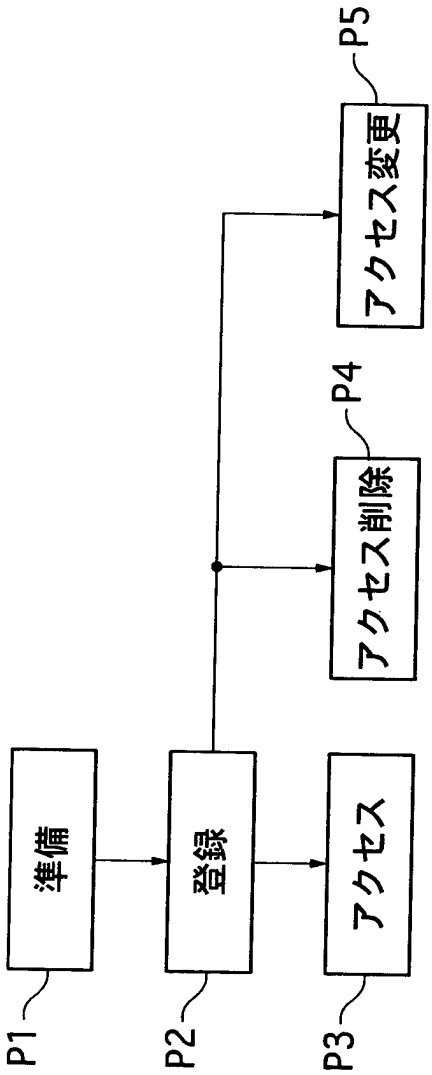
属性証明書のフォーマットの説明図

【図１０】



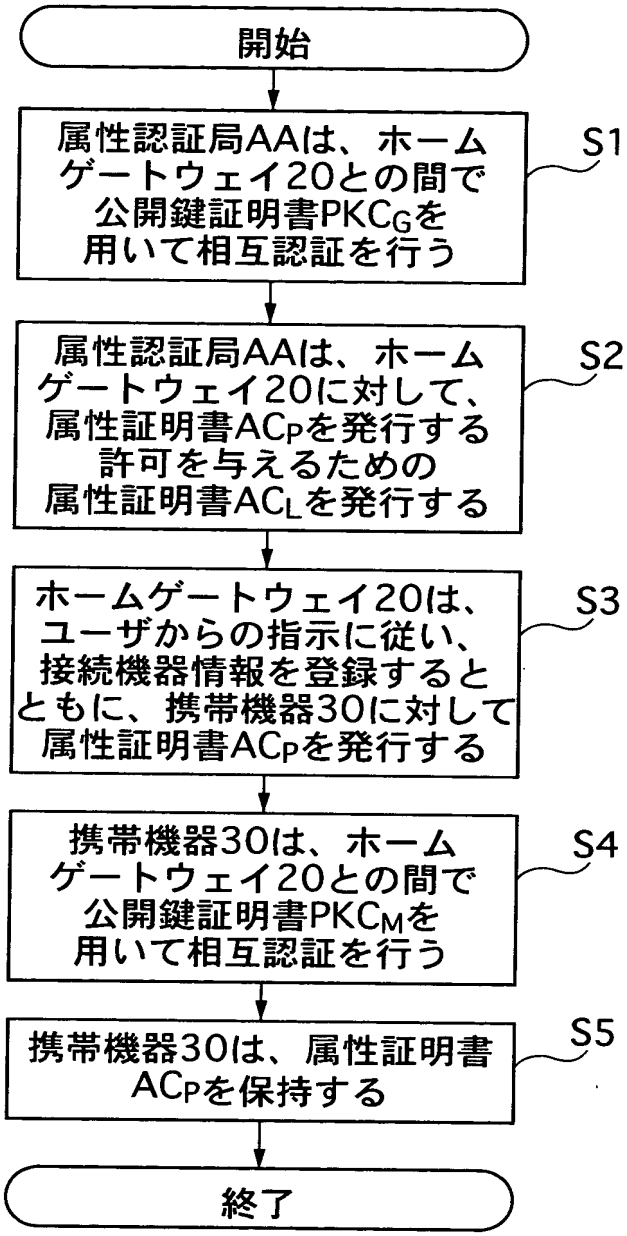
プロシキ情報の内容

【図１１】



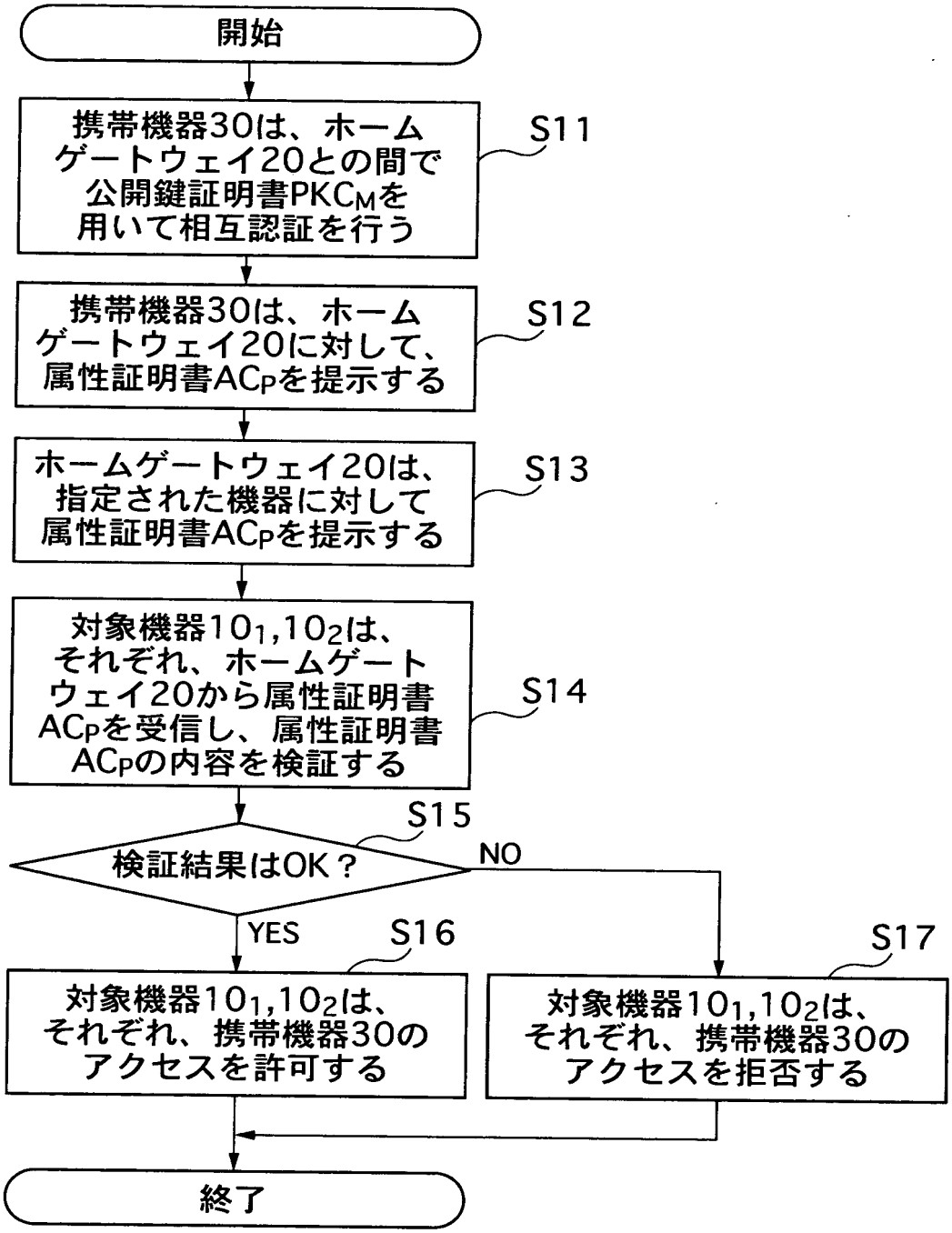
リモートアクセスシステムにおける一連の処理工程

【図１２】



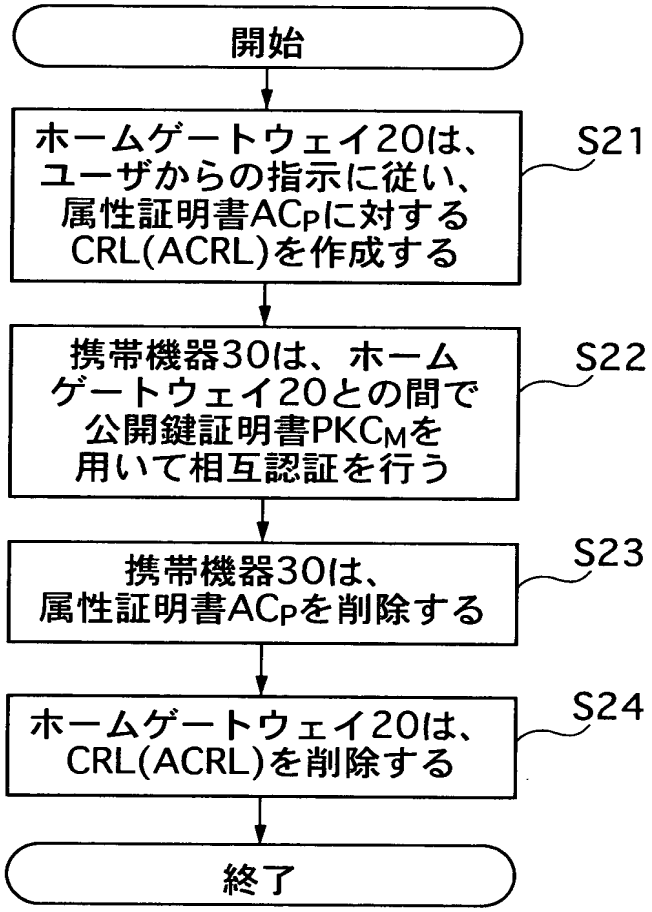
リモートアクセスシステムにおける一連の処理工程

【図１３】



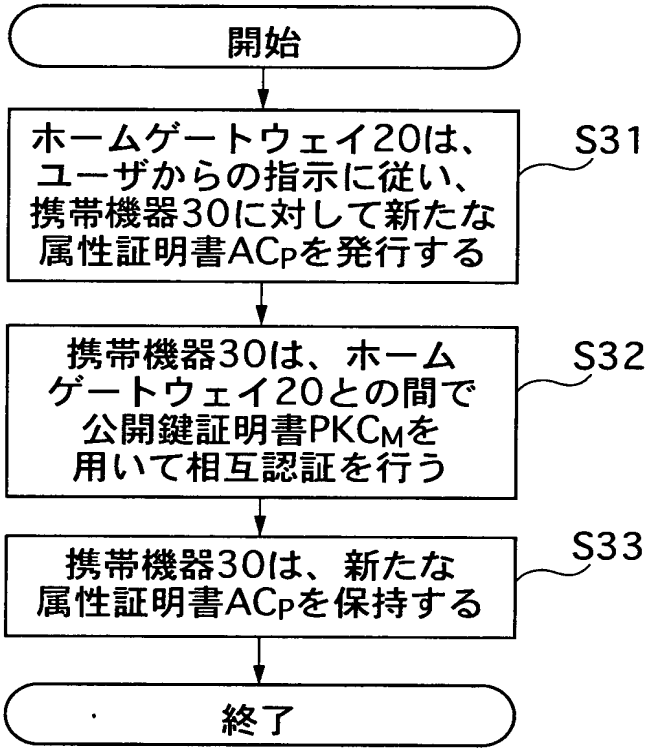
リモートアクセスシステムにおける一連の処理工程

【図１４】



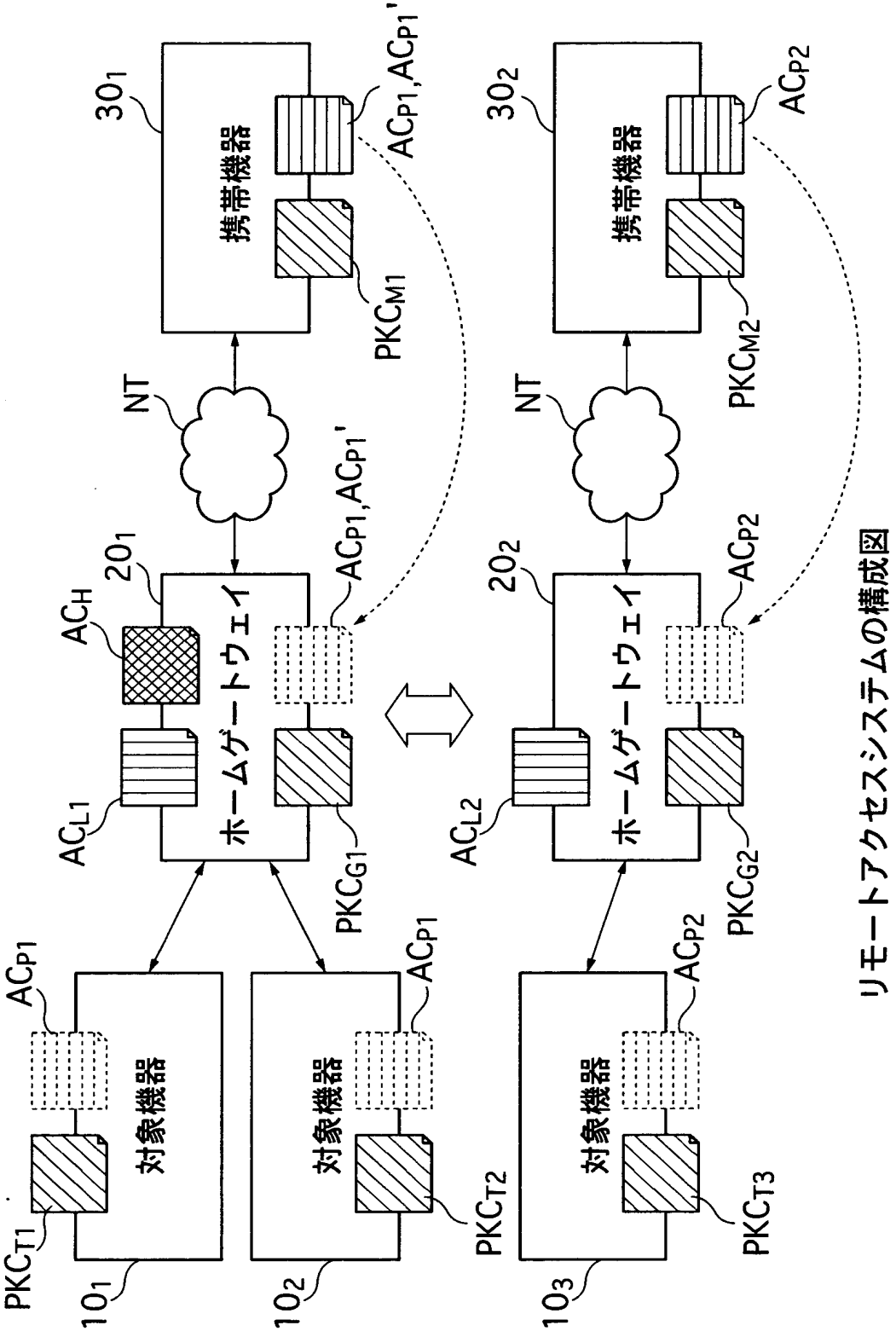
リモートアクセスシステムにおける一連の処理工程

【図１５】



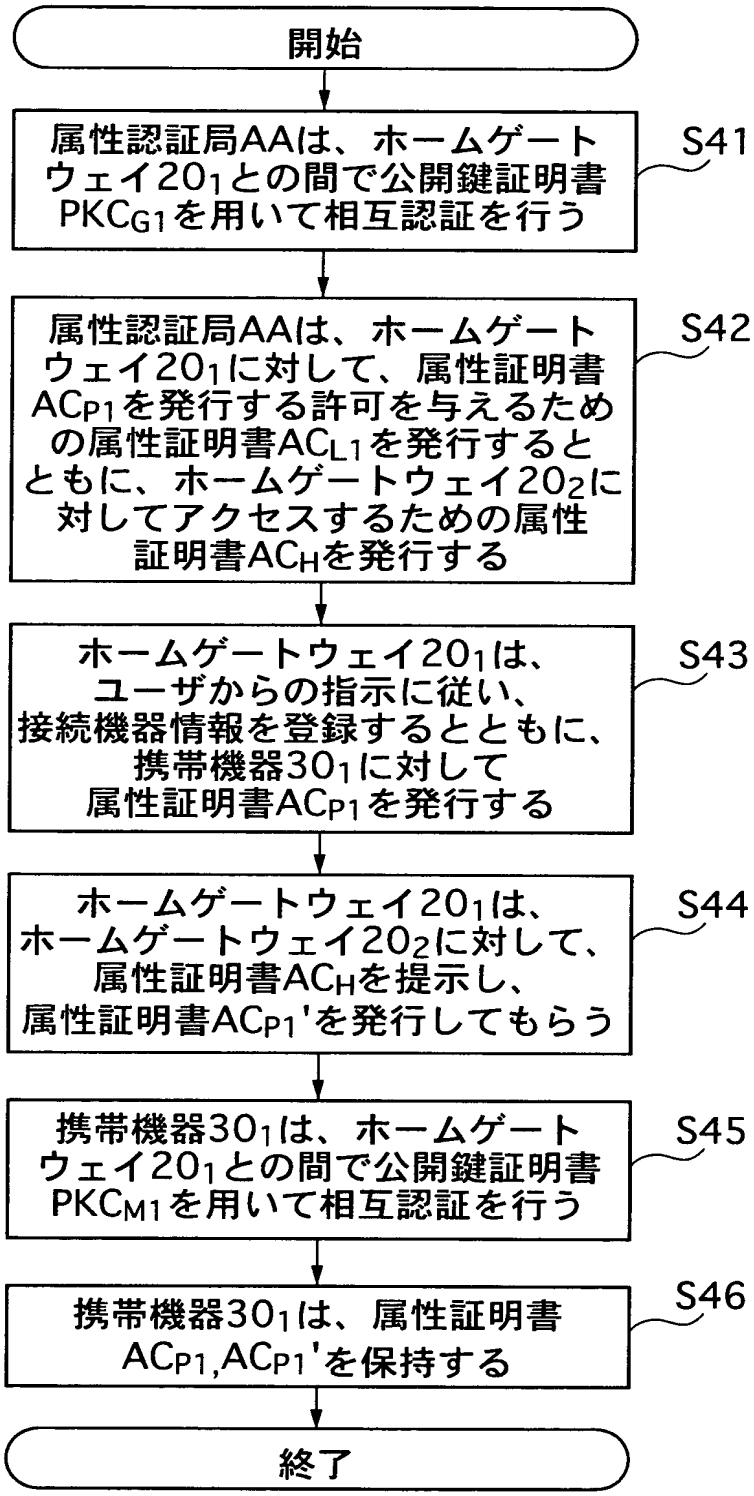
リモートアクセスシステムにおける一連の処理工程

【図１６】



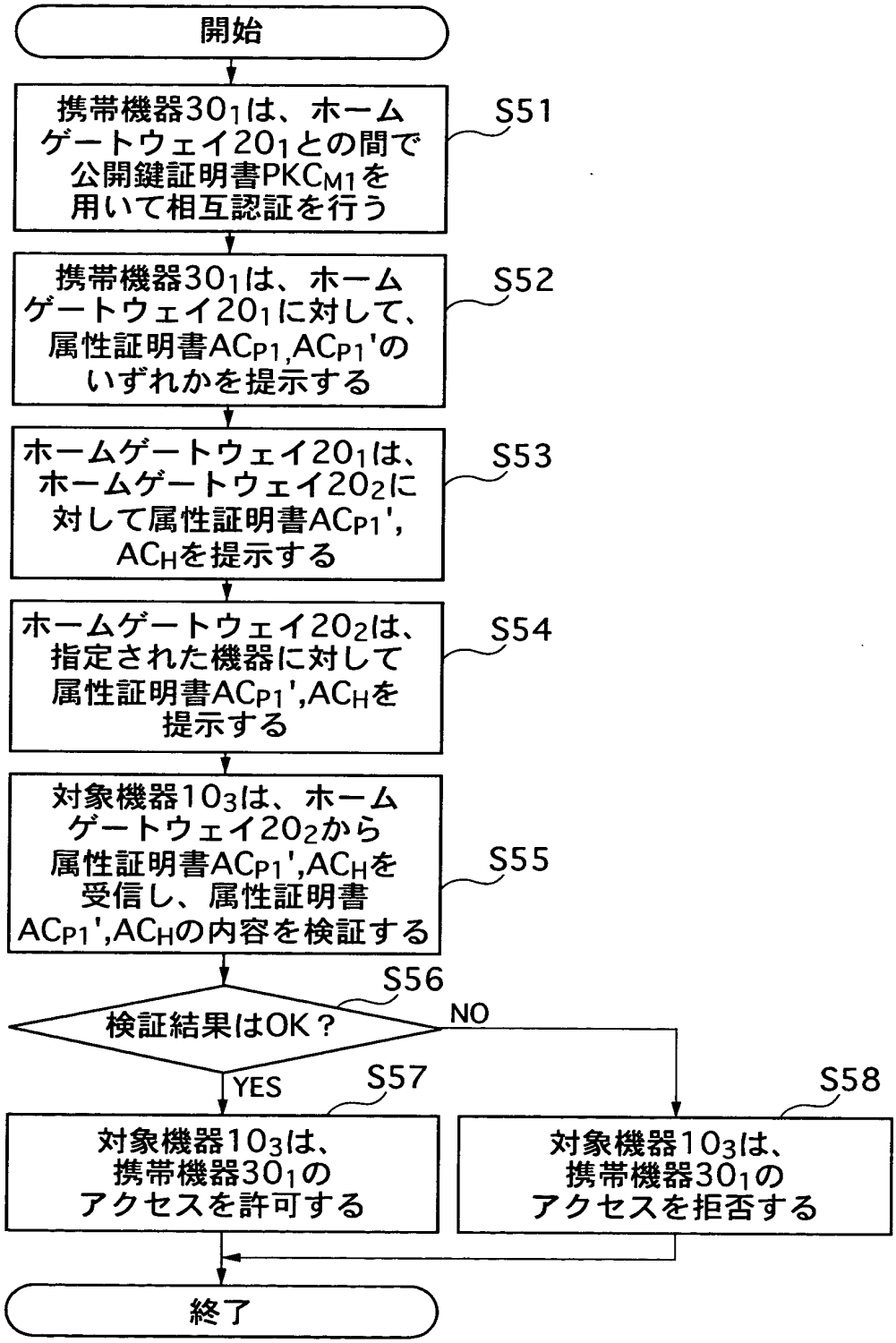
リモートアクセスシステムの構成図

【図１７】



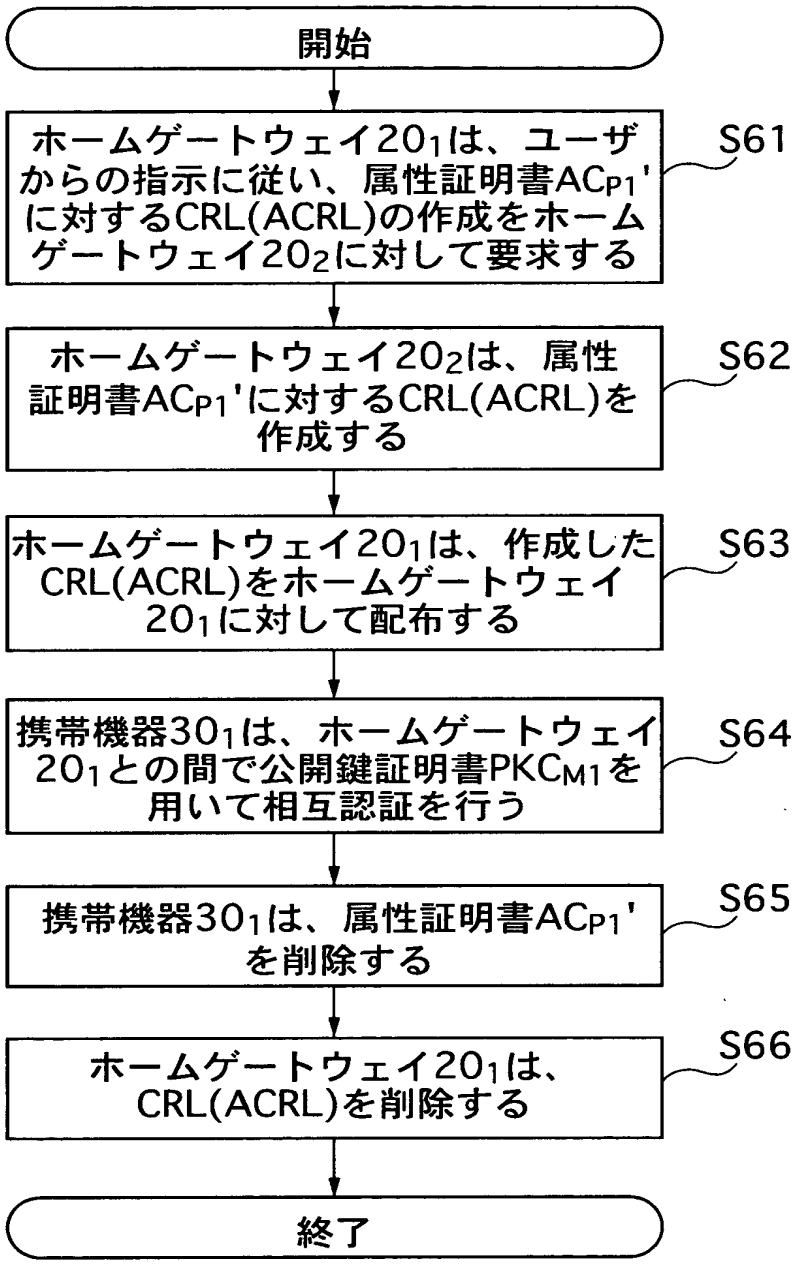
リモートアクセスシステムにおける一連の処理工程

【図１８】



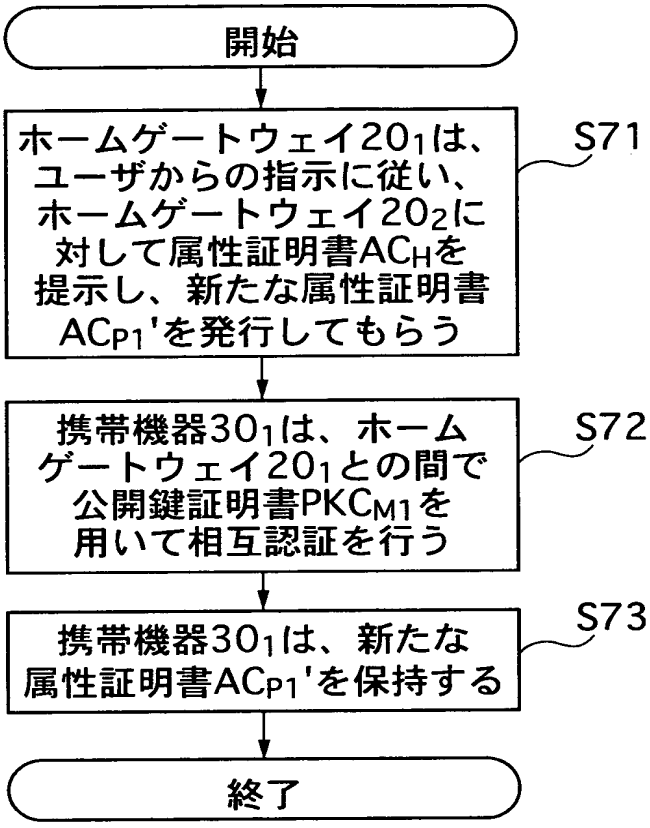
リモートアクセスシステムにおける一連の処理工程

【図１９】



リモートアクセスシステムにおける一連の処理工程

【図２０】



リモートアクセスシステムにおける一連の処理工程

【書類名】　要約書

【要約】

【課題】　リモートアクセスを行う際に、アクセスさせたいリソース毎に、権限単位での制御を容易且つ安全に行う。

【解決手段】　リモートアクセスシステムは、アクセスの対象となる対象機器１０$_1$，１０$_2$と、これらの対象機器１０$_1$，１０$_2$が属する家庭内ネットワークの入り口に相当する機器であるホームゲートウェイと２０と、対象機器１０$_1$，１０$_2$に対してアクセスするためにユーザが所持する携帯機器３０とを、エンティティとして備える。リモートアクセスシステムにおいては、携帯機器３０が、少なくともリソースに対する権限と経由させるホームゲートウェイ２０の情報とが記述された属性証明書ＡＣ$_P$を、ホームゲートウェイ２０を介して対象機器１０$_1$，１０$_2$に対して送信して提示することにより、リソースに対する携帯機器３０のアクセスを検証する。

【選択図】　図６

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社